FIRST DRAFT

CLOUD SERVICE PROVIDER (CSP) SECURITY REQUIREMENTS GUIDE (SRG)

Version 1, Release 0.1

21 August 2023

Developed by DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Cloud Service Provider Security Requirements Guide (SRG) provides the security controls and requirements necessary for implementing cloud-based solutions. This SRG is left in a document format because it is primarily targeted to giving DOD-specific guidance to cloud service providers (CSPs). Mission Owners should also review and comply with this document; however, technical requirements for Mission Owners are specified in the Cloud Computing Mission Owner SRG.

Appendices A through D contain essential tables and summaries that aid in the understanding and utility of all sections of this document. CSPs and Mission Owners should note that the key focus of the Cloud Computing SRG documents is adding the DOD organization-defined architecture, security control values, and processes required for cloud services implementations.

This Cloud Service Provider SRG is intended to meet the following scope:

- Provides security requirements and guidance to DOD and commercial CSPs (DOD contractors) that want to have their cloud service offering (CSO) included in the DOD Cloud Service Catalog.
- Establishes a basis on which DOD will assess the security posture of a DOD or non-DOD CSP's CSO, supporting the decision to grant a DOD Provisional Authorization (PA) that allows a CSP to host DOD missions.
- Establishes a basis on which a DOD component's Authorizing Official (AO) will assess the security posture of a DOD CSP's CSO, supporting the decision to grant a DOD component's Authority to Operate (ATO) for the CSP/CSO, and a DOD PA if the CSO might be leveraged by other DOD components. (e.g., DISA's ATO/PA for milCloud).
- Defines the requirements and architectures for the use and implementation of DOD or commercial cloud services by DOD Mission Owners.
- Provides guidance to DOD Mission Owners, Security Control Assessors (SCAs), AOs, and others in planning and authorizing the use of a CSO.
- Supports the DOD Chief Information Officer's (CIO) Cloud initiative to migrate DOD websites and applications from physical servers and networks within DOD networks and data centers into lower-cost commodity IT services, which typically include virtual servers and networks that are an integral part of most cloud services provided by both DOD and commercial CSPs.
- Supports the DOD CIO's and federal government's Data Center Reduction initiatives.

The target audience for this Cloud Service Provider SRG includes:

- Commercial and non-DOD federal government CSPs.
- DOD programs operating as a CSP.
- DOD components and Mission Owners using or considering the use of commercial/non-DOD and DOD cloud computing services.
- DOD risk management assessment officials and AOs.

This SRG does not address all DOD systems and applications unless they are migrating to or leveraging DOD or non-DOD cloud services. It also does not address approved DOD or non-DOD systems and applications used by DOD that are already approved for direct access via the internet (not traversing the Defense Information Systems Network [DISN]) unless they are migrating to commercial cloud services directly accessed via the internet. While this SRG may be used to assess/approve such cloud services and the applications that use them, it is not intended to change the approved network access or connectivity methods they use.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.2.1 Relationship to Security Technical Implementation Guides (STIGs)

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include but is not limited to Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

1.3 SRGs/STIGs

SRGs are collections of security requirements applicable to a given technology family, product category, or an organization in general. SRGs provide nonproduct-specific requirements to mitigate sources of security vulnerabilities commonly encountered across IT systems and applications.

While the SRGs define the high-level requirements for various technology families and organizations, the STIGs are the detailed guidelines for specific products. STIGs provide product-specific information for validating, attaining, and continuously maintaining compliance with requirements defined in the SRG for that product's technology area.

Newly published SRGs and STIGs generally consist of a technology/product overview document and one or more Extensible Markup Language (XML) (.xml) files in Extensible Configuration

Checklist Description Format (XCCDF) containing the security requirements. Security requirements are presented in the form of CCIs and include product-specific configuration and validation procedures. Requirements in this Cloud Service Provider SRG are not being published in an XCCDF XML format at this time.

The security requirements contained within SRGs and STIGs, in general, are applicable to all DOD-administered systems, all systems connected to DOD networks, and all systems operated and/or administrated on behalf of the DOD. This requirement remains in force for all Mission Owners building systems in a cloud service. CSP systems must comply with configuration guidance consistent with the NIST SP 800-53 control CM-6 by using STIGs/SRGs or a configuration guide deemed equivalent by DOD.

1.4 SRG and STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

Some content requires a DOD Public Key Infrastructure (PKI) certificate for access. The Cyber Exchange website does NOT currently accept External Certificate Authority (ECA) certificates for entry into the PKI-protected area. Industry partners needing PKI-restricted content may request it through their DOD sponsor.

1.5 Document Revisions and Update Cycle

The DISA Risk Management Executive, Cybersecurity Standards Branch, develops, revises, updates, and publishes SRG and STIG documents on a quarterly maintenance release schedule as needed. These publications reflect new or changed policies, requirements, threats, or mitigations; reorganized content; corrected errors; and/or additional clarity. The release schedule can be found at https://cyber.mil/stigs/release-schedule/.

Major updates to an SRG or STIG result in a version change rather than an incremental release. New SRGs and STIGs and major updates will be released as soon as they are approved and ready for publication at any time during the year.

1.5.1 Comments, Proposed Revisions, and Questions

Comments, proposed revisions, and questions are accepted at any time via email at disa.stig_spt@mail.mil.

The DISA Risk Management Executive, Cybersecurity Standards Branch, coordinates all change requests with relevant DOD organizations before inclusion and subsequent publication in a maintenance release or major update.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made based on the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level because some settings may not be configurable in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). DOD AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS REQUIRED FOR SRGS

2.1 NIST SP 800-53 Requirements

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG and/or addressed via FedRAMP requirements. CNSSI 1253 defines the required controls for DOD systems based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.2 General Procedures

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.

2.3 Security Assessment Information

This Cloud Service Provider SRG, in support of DODI 8510.01, establishes the DOD security objectives to host DOD mission applications and DOD information in internal and external IT services in the form of CSP's CSOs. The sensitivity of the DOD information may range from publicly releasable up to and including SECRET. Missions above SECRET must follow existing applicable DOD and policies and are not covered by this Cloud Service Provider SRG.

The intelligence community offers approved cloud services at classification levels above SECRET. Contact the DOD CIO Cloud team for additional information at: osd.cloudcomputing@mail.mil . This Cloud Service Provider SRG applies to all CSPs/CSOs hosting DOD systems, information, data, or applications, regardless of who owns or operates the environments. Mission Owners/operators can be DOD components, federal government agencies, or commercial entities.

CSPs not operated by the Mission Owner are essentially "a contractor of an agency" that operates an information system on "behalf of an agency." Mission Owners contracting with a CSP are outsourcing all or a portion of their information technology workloads to the CSP.

Mission Owners must comply with the requirements in the Cloud Computing Mission Owner SRG as well as any applicable requirements in this document. Thus, this document also applies to all DOD Mission Owners using cloud services and all parties involved in the provisioning of cloud services to DOD Mission Owners. This includes integrators or brokers and CSPs serving as a prime contractor as well as any supporting third-party CSO, CSP, or facilities provider (i.e., subcontractor) that an integrator/broker/CSP might leverage or contract with to provide a complete service or set of services under a DOD contract. For example, if CSP A instantiates its Software as a Service (SaaS) offering in CSP B's Infrastructure as a Service (IaaS) offering, which is in CSP C's data center, the Cloud Service Provider SRG is applicable to all three CSP/CSO entities for the applicable requirements. Similarly, for a cloud services integrator/broker that uses or resells one or more CSPs/CSOs to fulfill contract requirements, the Cloud Service Provider SRG is applicable to all cloud services.

While DODI 8510.01, DOD RMF, requires that IT services and IT products be assessed but not authorized, the risks of using cloud computing require a different approach. The DOD CIO has determined that a two-step authorization process is required. The first step is to assess the CSP's CSO to determine if it is secure enough to host DOD information and then preliminarily authorize or preapprove the CSO through the development of a DOD PA. This process is primarily for commercial CSOs. The second step is for the Mission Owner's (i.e., the DOD customer of the CSO) AO to be aware of the risk to their specific information by the specific cloud use case and to accept that risk through an ATO.

Although the CSP's overall service offering may be inheriting controls and compliance from a third party, the prime CSP (i.e., the CSP or integrator with a DOD contract for service), is ultimately responsible for complete compliance. This applicability statement and associated requirements are consistent with DOD and federal acquisition requirements and clauses, which state that DOD contractors (in this case integrators/brokers/CSPs) must include all security requirements incumbent upon them in all subcontracts.

The authorization process for commercial and non-DOD CSPs is based on Federal Information System Management Act (FISMA) and NIST RMF processes using FedRAMP, supplemented with DOD in this SRG. These requirements and considerations are a subset of the requirements in the DOD RMF. The authorization process for DOD enterprise service programs providing cloud capabilities or service offerings (e.g., milCloud, Defense Enterprise Email) is based on the DOD RMF requirements and processes, which are similar to the FISMA and NIST RMF processes. Both use baselines similar to the NIST SP 800-53 security controls as the foundation of the assessment, providing a common framework under which DOD can determine the level of risk.

This SRG establishes the DOD baseline security requirements for DOD Mission Owners when contracting for and using a non-DOD SaaS offering and when implementing their systems and applications on DOD or non-DOD IaaS and Platform as a Service (PaaS) offerings.

- Because IaaS and PaaS involve CSP customers building a system or application on top of these service offerings, the release of this Cloud Service Provider SRG considers IaaS and PaaS as being similar and treats them in the same manner unless stated otherwise.
- SaaS is addressed to the extent of the other service models, with specific application requirements being identified in other application-related SRGs and STIGs.
- PaaS CSOs can range from very close to IaaS (where the Mission Owner is provided with only a few unsecured programming environments and an operating system that the Mission Owner must secure) to very close to SaaS (where the CSO is a mostly complete application for which the Mission Owner can only customize its interface).

While the cloud computing requirements apply to all DOD use cases of cloud computing, one of its primary focus points is facilitating the migration of DOD systems and applications hosted on physical infrastructure (virtualized or not) owned by DOD components and connected to DOD DISN services (i.e., Non-Secure Internet Protocol Router Network [NIPRNet] and Secret Internet Protocol Router Network [SIPRNet] to DOD or non-DOD cloud services).

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

This section outlines several concepts, terms, and supporting processes, providing a primer for the remainder of this document.

This Cloud Service Provider SRG introduces terminology and concepts that are unique to cloud computing and DOD's use of the technology. Because cloud terminology is essential to understand DOD requirements but is often used in different ways by vendors, these terms are defined in Appendix B: Glossary.

3.1 Key Terminology

The following is a list of key terminology used throughout this document:

- Cloud service provider (CSP).
- Commercial CSP.
- DOD CSP.
- Non-DOD CSP.
- Cloud service offering (CSO).
- DOD Cloud Service Catalog.
- DOD component.
- Mission Owner (MO).
- DOD Private CSO.
- Security controls (indicates controls or control enhancements).
- DOD off-premises.
- DOD on-premises.
- DOD virtually on-premises.

3.2 Cloud Computing, Cloud Service, and Cloud Deployment Models

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be provisioned and released rapidly with minimal management effort or service provider interaction.

The NIST-defined cloud service models include SaaS, PaaS, and IaaS. The NIST-defined deployment models are private, public, community, and hybrid clouds. DOD private/community cloud is a cloud service that is built for the exclusive use of DOD users or tenants. Federal government community cloud includes both DOD and other federal government tenants. For example, a cloud used exclusively by Army and Air Force tenants would be considered DOD private/community, while one used by DISA and the Department of State would be a federal government community cloud.

While vendors may market and name their offerings as they wish, DISA will categorize them into one of the above NIST cloud service models when listing them in the DOD Cloud Service Catalog.

Vendors are encouraged to market their services using the NIST cloud service model terminology. Service offerings that provide data storage without also providing computing services will be a subset of IaaS. Any other service models proposed by the vendor (such as Data as a Service) will have to be aligned to one of the three standard service delivery models and meet the appropriate controls. As used in this SRG, the terms "cloud computing" and "cloud services" refer to a service offering from a provider organization to one or more organizational customers or tenant organizations. These terms do not refer to classic forms of IT services delivery where organizations employ or assemble dedicated hardware (whether virtualized or not) for their own use. A service offering from a provider organization to a customer must be part of the construct.

3.3 CSP and CSO

A CSP is an entity that offers one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third-party facilities such as data centers, carrier hotels/collocation facilities, and Internet Exchange Points). CSPs offering SaaS may leverage one or more third-party CSOs (i.e., for IaaS or PaaS) to build out a capability or offering.

A CSO is the actual IaaS/PaaS/SaaS solution available from a CSP. This distinction is important since a CSP may provide several different CSOs.

3.4 FedRAMP

FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the federal government. The Office of Management and Budget mandates that all federal agencies use FedRAMP as their systems and applications are migrated to the commercial cloud under the federal government's Cloud First initiatives. As with all federal departments and agencies, DOD is required to use FedRAMP-approved CSPs and share Agency ATOs with the FedRAMP Secure Repository.

The FedRAMP Joint Authorization Board (JAB) is the primary governance and decision-making body for the FedRAMP program. JAB-approved standards and processes result in the award and maintenance of a PA to host federal government missions.

DOD leverages FedRAMP JAB PAs and non-DOD federal agency ATO packages residing in the FedRAMP Secure Repository, including all supporting documentation, when assessing a CSO for a DOD PA. However, DOD will only accept non-DOD Agency ATOs where the CSP/CSO was assessed by a FedRAMP accredited third-party assessment organization (3PAO). The American Association for Laboratory Accreditation (A2LA) accredits FedRAMP 3PAOs, with the FedRAMP Program Management Office (PMO) providing final approval.

3.5 FedRAMP+

FedRAMP+ is the concept of leveraging the work done as part of the FedRAMP assessment and adding specific security controls with adjusted parameter values or adjusted parameter values necessary to meet and ensure DOD's critical mission requirements. A CSP's CSO can be assessed in

accordance with the criteria outlined in this SRG, with the results used as the basis for awarding a DOD PA. Refer to Appendix D: FedRAMP+ Security Controls and Parameter Values.

3.6 DOD Provisional Authorization

A DOD PA is an acknowledgement of risk based on an evaluation of the CSP's CSO and the potential for risk introduced to DOD networks. DOD PAs are granted at all information Impact Levels. A PA provides a foundation that AOs responsible for mission applications must leverage in determining the overall risk to the missions/applications that are executed as part of a CSO.

A DOD PA is granted to the CSP for a specific CSO, not the CSP itself. Furthermore, if a CSO leverages another CSP's CSO, the DOD PA includes inherited compliance. For example, if CSP A instantiates its SaaS offering in CSP B's IaaS offering, then CSP A's CSO included the inherited compliance of CSP B. Alternately, CSP A offering an SaaS leverages CSP B, CSP C, and CSP D to provide various functionality for its service offering, and then CSP A inherits CSP B's, C's, and D's security posture (compliance or noncompliance).

In both cases, CSP A will be contractually responsible for CSP B and must have accountability for controls in its subcontracts. It is therefore highly recommended that CSPs offering service to DOD only use other CSOs that have a DOD PA. If a leveraged CSO does not have a PA, it will be assessed as part of the primary CSO. However, such subtended assessments will not automatically grant the leveraged CSOs an independent PA. CSPs must disclose subcontracted CSOs used in the CSOs offered to DOD when assessed for a DOD PA.

While vendors/developers/integrators/CSPs that offer an SaaS CSO instantiated on a third-party I/PaaS CSO that has a FedRAMP P-ATO and a DOD PA (e.g., Amazon Web Services [AWS], Microsoft Azure, etc.) inherit security control compliance from that CSO, the SaaS must still be assessed and approved for its own DOD PA (usually this includes a FedRAMP P-ATO) if it is to be used by the DOD. This is because the application itself must be assessed/approved since it must meet many of the same security control requirements that the underlying CSO must meet.

DOD PAs are not granted to physical facilities (e.g., a data centers) that support cloud infrastructure even if the facility might be considered a CSO if it supports multiple CSPs or multiple tenants' equipment. These are assessed for the physical and environmental controls as part of the CSP's CSO by the 3PAO for unclassified facilities. Classified processing facilities are addressed in the Facilities Requirements section.

A DOD PA is revocable if a CSP/CSO loses its FedRAMP PA or if the CSP does not maintain compliance with its security responsibilities identified in this Cloud Service Provider SRG, associated requirements in other referenced documents, or contract requirements. Additionally, a CSP's CSO with a DOD PA that leverages another CSP's CSO with a DOD PA may lose its PA if the leveraged CSO loses its PA. CSPs acting as prime contractor must maintain the PA for their CSO and require all subcontracted CSPs to maintain the PA for their CSOs for the term of the contract. This flow-down is also applicable to cloud services integrators and brokers acting as prime contractors. If a prime or subcontracted CSO loses a PA and refuses to correct or cannot correct the reason(s) for it, such a condition may constitute a breach of contract. Revoking a PA is an extreme measure, and DOD will work with the CSP to resolve the issues leading to revocation. The DISA AO is responsible for approving and revoking DOD PAs.

CSOs possessing a DOD PA are listed in the DOD Cloud Service Catalog. DOD component services may also implement approved CSP/CSO listings for their agency's use.

3.7 Information Impact Levels

Cloud security information Impact Levels are defined by the combination of:

- The sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and
- The potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information.

DOD Mission Owners must categorize mission information systems in accordance with DODI 8510.01 and CNSSI 1253 and then identify the Cloud Information Impact Level that most closely aligns with the defined categorization and information sensitivity. This process leverages the FedRAMP Moderate or High baselines through reciprocity.

The security control baseline for Impact Levels 2 and 4 is based on moderate confidentiality, integrity, and availability (i.e., MMM). National Security Systems and Impact Levels 5 and 6 are based on high confidentiality, integrity, and availability (i.e., HHH). If a Mission Owner has high potential impacts, specific requirements must be included in the contract/SLA to address/mitigate this risk or deploy to DOD facilities assessed using CNSSI 1253 high baselines through the DOD RMF. The Mission Owner is expected to assess the CSO's stated availability rating(s) during CSP selection. Any specific or additional availability requirements must be included in the contract or a service-level agreement with the CSO.

CSOs will be evaluated as part of the assessment process for availability. The assessed level of availability will be listed in the DOD Cloud Service Catalog. This evaluation does not prevent a CSO from receiving a PA or being included in the DOD Cloud Service Catalog; it is only used to facilitate the matching of a DOD Mission Owner to one or more appropriate cloud services meeting their needs.

DOD Impact Levels segregate major types of information into "buckets" depending on the information's audience and sensitivity. This requires different protections and treatments than the basic RMF information categorization of Low, Moderate, and High used by FedRAMP. For example, the FedRAMP baselines do not address National Security Systems/Information or classified information, which is under the purview of the Committee on National Security Systems (CNSS).

Impact Levels do not apply to FedRAMP baselines. Impact Levels are a DOD construct only. It is inaccurate to refer to a DOD PA for a given DOD Impact Level as a FedRAMP Impact Level number.

3.7.1 Impact Level 2: Noncontrolled Unclassified Information

Impact Level 2 accommodates publicly releasable data or nonpublic unclassified data where the unauthorized disclosure of information could be expected to have a limited adverse effect on

organizational operations, organizational assets, or individuals. This includes all data cleared for public release as well as some low confidentiality unclassified information NOT designated as Controlled Unclassified Information (CUI) or military/contingency operations mission data, but the information may require some minimal level of access control (e.g., user ID and password). This Impact Level accommodates non-CUI information categorizations based on CNSSI-1253 at moderate confidentiality, integrity, and availability.

Commercial Impact Level 2 CSP/CSO customers include whomever the CSP chooses to market the CSO to, which may include government customers, commercial customers, and the public. Access to the CSO is via the internet.

3.7.2 Impact Level 4: Controlled Unclassified Information

Impact Level 4 accommodates nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This encompasses CUI and/or other mission data, including that used in direct support of military or contingency operations. CUI is information the federal government creates or possesses that a law, regulation, or governmentwide policy requires, or specifically permits, an agency to handle by means of safeguarding or dissemination controls.

CUI requires protection from unauthorized disclosure. CUI does not include classified information or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from an executive branch agency or entity acting for an agency. Designating information as CUI or mission data to be protected at Impact Level 4 is the responsibility of the owning organization. Determination of the appropriate Impact Level for a specific mission with CUI and mission data will be the responsibility of the mission AO. Some types of CUI may not be eligible to be hosted on Impact Level 4 CSOs without additional assessment over and above the DOD PA. (e.g., for privacy or classified). This Impact Level accommodates CUI information categorizations based on CNSSI-1253 up to moderate confidentiality, integrity, and availability (MMM).

Impact Level 4 CSOs may support a U.S. government community or a DOD-only community (i.e., the CSO is DOD Private).

Commercial Impact Level 4 CSP/CSO customers include all U.S. government customers (federal, state, local, and tribal) and commercial customers that support them. In some cases, an Impact Level 4 PA may be granted to CSOs that support other commercial entities but not the public. Commercial Impact Level 4 CSO customers include the following:

- DISN NIPRNet-based DOD components – DOD components whose primary network connection to other DOD components and the internet is via NIPRNet. Such DOD components' primary internet access is via the DISN NIPRNet Internet Access Points (IAPs).
- DOD contractors operating a system or application for the DOD. This is primarily for the fulfillment of the contract, not for the contractor's general storage/processing of CUI/Covered Defense Information (CDI) or the contractor's internal corporate cloud use cases. In this case, the contractor is operating on the behalf of a Mission Owner and must fulfill all Mission Owner requirements as specified in the Cloud Service Provider SRG.

- NIPRNet connected but separate community of interest (COI) Mission Partner networks, e.g., MedCOI, DREN.
- Non-NIPRNet-based DOD components, e.g., Commissary, .edu organizations.
- Federal, state, local, and tribal government agencies.
- DOD contractors required to store/process DOD CUI or CDI as part of their DOD contract. This is primarily for the fulfillment of the contract, not for the contractor's internal corporate cloud use cases.

Impact Level 4 customer CSO connectivity:

- NIPRNet-based DOD components connect via DOD-provided, DOD CIO-approved NIPRNet boundaries and associated private connectivity.
- Non-NIPRNet-based DOD components connect via DOD component-provided, DOD CIO-approved, and non-NIPRNet boundaries and associated private connectivity. Alternate connectivity methods must be approved by DOD CIO.
- All other CSO customers establish their own boundaries and private or internet-based connectivity.

3.7.3 Impact Level 5: Controlled Unclassified Information and Unclassified National Security Information (U-NSI)

Impact Level 5 accommodates nonpublic, unclassified NSS system data (i.e., U-NSI) or nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. This includes CUI and/or other mission data that may require a higher level of protection than that afforded by Impact Level 4 as deemed necessary by the information owner, public law, or other government regulation. The determination of whether CUI and/or mission data fits this category is up to the AO responsible for categorizing the information and choosing the Cloud Impact Level.

Because NSS-specific security requirements are included in CNSSI 1253, U-NSS information must be implemented in Impact Level 5 CSOs.

This Impact Level accommodates NSS and CUI information categorizations at CIA HHH. Per CNSSP 32, the minimum requirement for all unclassified NSS is equivalent to the FedRAMP High baseline. Impact Level 5 CSOs may support DOD private clouds such as a federal government community or DOD-only community. Examples of this include the following:

- DISN NIPRNet-based DOD components i.e., DOD components whose primary network connection to other DOD components and the internet is via the DISN unclassified network service called NIPRNet. Such DOD components' primary internet access is via the DISN NIPRNet IAPs.
- NIPRNet connected but separate COI Mission Partner networks, e.g., MedCOI, DREN.
- Non-NIPRNet-based DOD components, e.g., commissary, .edu organizations.
- Federal agencies operating an unclassified NSS.
- Federal agency and DOD contractors operating a system or application (including an unclassified NSS) for the federal agency or DOD. This is primarily for the fulfillment of the

contract, not for the contractor's general storage/processing of CUI/CDI or the contractor's internal corporate cloud use cases. In this case, the contractor is operating on behalf of a Mission Owner and must fulfill all Mission Owner requirements as specified in the Cloud Service Provider SRG.

Impact Level 5 customer CSO connectivity:

- NIPRNet based DOD components connect via DOD-provided, DOD CIO-approved NIPRNet boundaries and associated private connectivity.
- Non-NIPRNet-based DOD components connect via DOD component-provided, DOD CIO-approved, non-NIPRNet boundaries and associated private connectivity. Alternate connectivity methods must be approved by DOD CIO.
- All other CSO customers establish their own boundaries and private or internet-based connectivity.

3.7.4 Impact Level 6: Classified Information up to SECRET

Impact Level 6 accommodates nonpublic, classified NSS system data (i.e., classified National Security Information [NSI]) or nonpublic, unclassified data where the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. At this time, only information classified as SECRET or below, in accordance with the applicable executive orders, is permitted to be hosted at this Impact Level. Access to the CSO is via one or more private SIPRNet connections.

Impact Level 6 accommodates classified information categorizations (HHH). Impact Level 6 CSOs may support a federal government community or a DOD-only community (i.e., the CSO is DOD Private). Due to the requirement that the entire CSO infrastructure be dedicated and separate from other CSP/CSO infrastructure, Impact Level 6 CSOs may only be provided by CSPs under contract to the DOD or a federal agency. In this sense, the CSO is not considered "commercial" or "commercially available" even though the CSO infrastructure is expected to be an exact or close copy of the given CSP's commercial offering.

Impact Level 6 CSO customers include the following:

- DISN SIPRNet-based DOD components, i.e., DOD components whose primary network connection to other DOD components for SECRET classified communications is via the DISN SECRET network service called SIPRNet.
- Federal agencies whose networks are part of the National Secret Fabric and/or are connected to SIPRNet.
- SIPRNet-connected but separate COI Mission Partner SECRET networks; federal agency SECRET networks.
- DOD contractors operating a SECRET NSS for the DOD. This is primarily for the fulfillment of the NSS contract but might also be used (if approved) for the contractor's general storage/processing of SECRET CDI.

3.7.5 DOD Use of FedRAMP Security Controls

Impact Level 2: Components may host unclassified DOD information that has been publicly released on FedRAMP-approved cloud services. Impact Level 2 information may be hosted in a CSP that minimally holds a FedRAMP Moderate or High PA (subject to compliance with the personnel security requirements and acceptance by the Mission Owner and the responsible AO). Only FedRAMP Moderate or High baseline controls will be assessed for DOD PAs for Impact Level 2. DOD provides full reciprocity with FedRAMP Moderate and High P-ATOs for DOD Impact Level 2. This in no way alleviates the CSP from meeting other security and integration requirements for CSPs/CSOs as required by the Mission Owner while hosting DOD IT missions or the Mission Owner from securing their systems/websites/applications in Impact Level 2 CSOs.

Impact Level 4: The FedRAMP Moderate baseline, supplemented with DOD FedRAMP+ security controls and other requirements in this SRG, is used to assess CSPs toward awarding a DOD PA at information Impact Level 4.

An alternate path to a DOD Impact Level 4 PA is available due to coordination of the FedRAMP High baseline, DOD Impact Level 4 FedRAMP+ security controls, and other requirements in this SRG.

Impact Levels 5/6: The FedRAMP High baseline, supplemented with DOD FedRAMP+ security controls and requirements in this SRG, is used to assess CSPs toward awarding a DOD PA at information Impact Level 5/6.

No matter what security control baseline is used as the basis for a FedRAMP PA, additional considerations and/or requirements must be assessed and approved before a DOD PA can be awarded. These considerations and/or requirements can be found throughout this SRG.

4. RISK ASSESSMENTS AND AUTHORIZATION

The shift to cloud computing necessitates adjustments to the DOD Risk Management processes, which typically address physical on-premises systems and applications, to accommodate the use of commercial CSOs. The goal is to address the security requirements and controls in the cloud while ensuring the security of DOD's core missions and networks in accordance with the DOD RMF.

The DOD CIO has determined that a two-step authorization process is required when leveraging commercial CSOs. The first step is to assess the CSO to determine if it is secure enough to host DOD information. The CSO receives preapproval via the DOD PA. The second step is for the Mission Owner's (i.e., the DOD customer of the CSO) AO to be aware of the risk to their information by the commercial cloud use case and to accept that risk through an ATO.

The DOD PA risk assessment process is focused on evaluating the requirements for the Impact Levels that a CSO can support. The Mission Owner must choose a CSO that meets their operational needs and has a DOD PA at the information Impact Level corresponding to the categorization of the information being processed or stored in the CSO. The Mission Owner's AO must then leverage the PA and supporting documentation in granting the required ATO for the mission system operating within the cloud.

The following lists the relationship between DOD PA, Mission Owner's ATOs, and the associated CSOs:

- Commercially owned/operated on- or off-premises CSOs will be assessed for a DOD PA.
  - For I/PaaS, the Mission Owner must develop an assessment package for the application/system built on the CSO.
  - For I/PaaS, the Mission Owner's AO must accept the risk of hosting their information in the CSO based on the PA and the Mission Owner's assessment package.
  - For SaaS, the Mission Owner's AO must accept the risk of hosting their information in the CSO through the development of an ATO (unless an enterprise-level ATO exists for the CSO) based on the PA.
- Commercially owned/operated on- or off-premises CSOs designated by DOD CIO and DISA as an enterprise service will be assessed for a PA. If successful, an enterprise ATO will be awarded that any DOD component can leverage through reciprocity.
- Government-owned/operated or government-owned/contractor-operated on-premises CSOs will be awarded an ATO.
  - If designated by DOD CIO and DISA as an enterprise service, the CSO will be assessed and then awarded an enterprise ATO that can be leveraged by any DOD component through reciprocity.
  - If a DOD component owns the CSO infrastructure, the CSO will be assessed, and the component AO will award the ATO.

4.1 Commercial and Non-DOD Cloud Services for Enterprise Use

The requirements in this section pertain to commercial/non-DOD CSOs.

Impact Level 2: Information may be hosted in a CSP that is provisionally authorized as FedRAMP compliant at the moderate or high level through full reciprocity. The two acceptable government authorizations are:

- **C.1** JAB P-ATO – Based on a determination by the JAB that an acceptable level of risk exists for leveraging across the federal government. DOD/DISA is an active participant in the technical reviews of the JAB P-ATO security assessment artifacts.
- **C.2** FedRAMP-listed Agency ATOs – Based on an assessment and ATO issued by a federal government agency where the CSP was assessed by a FedRAMP accredited/approved 3PAO.

DOD will not require additional NIST 800-53 RMF control assessments at Impact Level 2. Any CSP/CSO compliant at the FedRAMP Moderate or High level may be used at DOD Level 2 without a written DOD PA. Thus, compliance with FedRAMP Moderate or High level is equivalent/essentially an automatic DOD Level 2 PA. If such a CSO becomes too risky for DOD use, DISA will rescind its automatic DOD Level 2 PA with a written memo.

If DOD components require a CSO with mission needs at Impact Level 2, but the CSO does not have a FedRAMP Moderate (or higher) JAB P-ATO or Agency ATO, they may assess and authorize the CSO. The DOD component can submit their ATO to FedRAMP for inclusion in the Marketplace.

Impact Level 4/5/6: DOD will leverage existing documentation and artifacts from previous FedRAMP-JAB or non-DOD Agency authorizations in the FedRAMP Secure Repository. Proprietary artifacts provided by the CSP will also be evaluated. FedRAMP+ requirements will be assessed by a FedRAMP accredited/approved 3PAO. After the validation of the Security Assessment Report (SAR), the DISA Cloud Security Control Assessor (SCA) organization will prepare an overall determination of risk to support a DOD PA decision. The DISA AO approves DOD PAs for the DOD CIO.

All reciprocity and/or non-DOD review for authorization will require the CSP security clearance policy to be checked. All CSPs are required to follow the security clearance requirements within this document in Section 5: Security Requirements.

DOD will provide reciprocity for Impact Level 4 from a FedRAMP High baseline via either agency or JAB ATO with the addition of general readiness requirements being assessed and security clearance policy review.

A DOD component must sponsor a CSP/CSO for a DOD Impact Level 4/5/6 PA. The Component sponsor must leverage NIST SP 800-53 C/CE to validate the CSP's CSO SAR. Application for sponsorship is accomplished through the DOD Cloud Authorization Services (DCAS) website.

The following three paths can be followed in assessing a CSO for an Impact Level 4/5 DOD PA:

1. **CSPs with a FedRAMP JAB PA or in the process of obtaining a JAB PA:** This is the DOD preferred path to a DOD PA because the DISA SCA and the DOD CIO have already been involved in the FedRAMP validation and authorization activities.

- DOD leverages the documentation and artifacts produced as part of the FedRAMP process, supplemented with an assessment of the DOD-specific security controls and requirements not addressed by FedRAMP for Impact Level 4 and above.
- CSPs having a FedRAMP JAB PA have been assessed by an accredited/approved 3PAO against the FedRAMP Moderate or High Baseline.
- For those in the process of obtaining a JAB PA, the DOD promotes the use of parallel activities (FedRAMP and FedRAMP+) to minimize cost and create efficiencies in the assessment process.

2. **FedRAMP-listed Non-DOD Agency ATO:** Mission owners, their AOs, and/or the DISA SCA must carefully assess Agency ATOs as the non-DOD agency may have accepted risks that are not appropriate for DOD to accept. This path is not available to CSOs having a DOD component. The DISA AO must sign and submit the DOD Agency to FedRAMP for the DOD CIO.

   - CSPs having a non-DOD federal agency authorization based on security controls assessed by an accredited/approved 3PAO can be assessed for a DOD PA provided the authorization is listed in the FedRAMP agency authorizations. The acceptable minimum baseline for NSS is FedRAMP Moderate and for all others, it is FedRAMP High.
   - The information from the non-DOD agency ATO will be supplemented with an assessment of the DOD-specific controls and requirements not addressed by FedRAMP for Impact Levels 4/5/6. This assessment should be performed by the CSP's 3PAO and submitted to the DISA SCA for review and validation toward awarding a PA.

3. **DOD component Assessed ATO leveraged for a DOD PA**: A DOD component assessment of a CSP's CSO for a DOD PA may be performed when a FedRAMP JAB P-ATO or a 3PAO non-DOD Agency ATO does not exist. The two circumstances when this would occur are:

   - If a DOD organization has a validated mission requirement that only the specific CSP's CSO can fulfill, requiring it to be authorized.
   - If a DOD organization acting as a CSP develops and instantiates a CSO.

   In these circumstances, the CSP's CSO are fully assessed by a FedRAMP and approved 3PAO in coordination with the DISA Cloud SCA organization:

   - In coordination with the DISA cloud security assessment team, DOD organizations are required to resource the full assessment of a CSP's CSO authorization. The assessment of the FedRAMP and other applicable SRG requirements determine whether the DISA AO will grant a DOD PA for the appropriate Impact Levels.
   - CSPs that receive a DOD-assessed PA will have their assessment package available in the FedRAMP Marketplace and the DOD Cloud Services Catalog. DOD PAs signed by the DISA AO serve as a DOD Agency ATO for FedRAMP reciprocity.
     - If the service offering will only be used by DOD customers, the CSP's assessment package will only be available through the DOD Cloud Service Catalog because private clouds are ineligible for inclusion in the FedRAMP catalog.
   - DOD CSP CSOs will be assessed for a full ATO (in accordance with the DOD RMF) and PA (in accordance with commercial CSP requirements in this SRG).

DOD PAs must be signed by the DISA AO for the CSO to be used by multiple DOD components (the enterprise) or serve as a DOD Agency ATO for submission to FedRAMP for use by other federal agencies. ATOs that are signed by a DOD component AO only permit the CSO to be used within that DOD component.

CSOs should be assessed for FedRAMP and DOD requirements simultaneously by the same 3PAO. This permits CSPs to avoid redundancies in assessments when they seek to have a CSO included in both the FedRAMP and DOD Cloud Service Catalog.

The DISA AO will review any change of ownership involving a CSP, whether the primary CSP or an underlying CSP on which a CSO was built, to assess the impacts and risks associated with the continuation of the DOD PA. DOD CIO, DISA AOs, and Mission Owners must be notified of any potential change to CSP ownership six months prior to the transition. This initiates the PA review process and allows sufficient time for Mission Owners to offboard and retrieve any necessary information/data from the current CSP. Mission Owners must address CSP ownership in their SLAs/contracts.

Impact Level 6 Off-Premises*:* An Assessment and Authorization (A&A) of an off-premises DOD contractor facility and subsequent information systems that process, store, and transmit classified information (i.e., non-DOD commercial CSPs and their Level 6 CSOs) must be performed in conjunction with the following policies and regulations:

- National Industrial Security Program (NISP) (as defined in Executive Order 12829).
- Title 48 Code of Federal Regulations (CFR) Subpart 4.4 – Safeguarding Classified Information within Industry.
- Federal Acquisition Regulations (FAR) Section 52.204-2 – Security Requirements.

NISP policies are the purview of the Office of the Undersecretary of Defense for Intelligence (OUSD[I]) Industrial Security division and, for DOD, the Defense Counterintelligence and Security Agency (DCSA). DODI 5220.22 assigns DOD responsibilities for administration of the NISP in accordance with Executive Orders 10865 and 12829 to ensure classified information disclosed to industry is properly safeguarded. NISP responsibilities for DOD components are found in the DODI 5220.22; whereas commercial CSPs with Level 6 offerings must adhere to the National Industrial Security Program Operating Manual (DOD 5220.22-M). Together, the NISP, NISPOM, and Office of the Designated Approving Authority (ODAA) Process Manual provide further guidance.

The DOD CIO intends for all CSPs and CSOs to be assessed against the same set of requirements and cybersecurity control baselines as defined in DODI 8510.01 – DOD RMF, CNSSI 1253-Security Categorization and Control Selection for National Security Systems, and this SRG. Requirements and processes supporting the authorization of off-premises Commercial CSPs and their CSOs for Impact Level 6 will be coordinated with OUSD(I) and DCSA as NISP policies and procedures are updated. Notwithstanding the above, Level 6 CSOs must be assessed using the FedRAMP High Baseline, CNSSI 1253 High, and NSS controls and appropriate overlays following the FedRAMP processes using a 3PAO to receive a DOD PA. DISA and DCSA will jointly validate the SAR.

Level 6 processes should mirror the processes for Levels 4 and 5 except for facility and personnel clearances. DCSA authorizes the required facility clearances and coordinates with DISA for the DOD PA. The Mission Owner is still responsible for producing their ATO for using and placing their classified information in the Level 6 CSO as they are with all other unclassified levels.

Impact Level 6 On-Premises*:* Assessment and authorization of on-premises Impact Level 6 CSOs (i.e., DOD- or DOD contractor-managed CSOs in a DOD data center) will be performed by DOD component SCAs in accordance with the DOD RMF for DOD classified facilities, applications, connection approval, and personnel.

- The CSO may receive a DOD PA if the CSO will be offered to DOD components other than the authorizing component and the CSO meets the standards defined in this SRG.
- If the on-premises CSO is managed by a commercial CSP or DOD contractor, the CSP/contractor will be required to maintain the appropriate facilities and personnel clearances.

To receive a DOD PA, DOD On-Premises Impact Level 6 CSOs will be assessed in accordance with the FedRAMP High Baseline, the Impact Level 6 FedRAMP+ security control, the CNSSI 1253 High and NSS controls, and appropriate overlays. Such CSOs may need to meet additional CNSSI 1253 security controls in the baselines associated with the categorization of the information to be processed/stored in the CSO.

4.1.1 On-Premises Commercially Owned and Operated CSOs

On-premises commercially owned/operated CSOs (e.g., milCloud2 IaaS/PaaS or other SaaS) intended as a DOD-wide enterprise service are subject to the requirements found in this SRG and the same security controls as commercial CSOs. Therefore, a DOD PA is required before going into production.

Similarly, on-premises commercially owned/operated CSOs instantiated by DOD components may be assessed and authorized under a Component ATO using the requirements found in this SRG and the same security controls as commercial CSOs. The component ATO will only permit the CSO to be used by that component. ATOs will not be considered for a DOD PA.

DOD components are not permitted to submit DOD PAs or component ATOs as a DOD Agency ATO for inclusion on the FedRAMP Marketplace. The DOD CIO represents DOD as the Agency in this capacity; thus, only DOD-assessed PAs/ATOs signed by the DISA AO (representing the DOD CIO) may be submitted to FedRAMP as an Agency ATO.

4.2 DOD-Owned CSOs and Enterprise Cloud Services Applications

DOD-owned/operated and government-owned/commercially operated CSOs (e.g., original milCloud IaaS/PaaS) are subject to the same requirements found in this SRG and the same security controls as commercial CSOs. The DOD CSO must be assessed against the aggregate baseline made up of the appropriate FedRAMP baseline Moderate, at a minimum, and the appropriate CNSSI 1253 baselines (as tailored) for the CSO. DOD-owned/operated CSOs require a full ATO, which may be used in lieu of a PA or to generate a PA that can be leveraged by Mission Owners and their AOs.

DOD enterprise service programs considered as cloud services under the SaaS model are subject to the DODI 8510.01 requirements and CNSSI 1253 baselines. These DOD-assessed programs are not subject for assessment through FedRAMP and do not share DOD ATOs with the FedRAMP secure repository.

4.3 CSP and Mission Owner Risk Management

Risk management must consider both the CSO and the supported mission (i.e., the Mission Owner's system or application). Each CSO must be granted a DOD PA to host DOD mission systems. The DOD PA and supporting documentation will then be used by the Mission Owner's risk management officials as a basis of reciprocity for the controls provided by the CSP. The controls will vary based on the service model (IaaS, PaaS, SaaS) and could also vary based on requirements such as privacy or classification controls. For additional "shared controls," both the CSO and the Mission Owner must address a requirement. The responsible AO leverages the PA information, supplemented with an assessment of the risks within the Mission Owner's responsibility, in granting an authorization to operate.

4.3.1 Authorization Boundaries

Cloud computing has two primary authorization boundaries. These are determined by the division of control between the CSP and Mission Owner and are defined as follows:

1. **The CSP and CSO Authorization Boundary:** This boundary consists of two parts, the CSP organization and the CSO, and is addressed by the FedRAMP and DOD PAs.
   - The CSP organization maintains the corporate network, such as operational/security policies and procedures, physical facilities, network(s), hardware server platforms, hypervisors, VMs, and applications. CSOs will inherit the residual risk and security controls implemented by the CSP.
   - The CSO includes the infrastructure directly supporting the CSO and the following for each service type:

Table 4-1: CSO Authorization Boundary Based on Service Type

Service Type	CSO Authorization Boundary
IaaS	• Includes the network, storage, computing platforms, and hypervisors that compose the IaaS service offering.
PaaS	• May build on the devices and platforms used in IaaS and includes the VMs, their operating systems, and platform applications. • Some, if not all, that are listed for IaaS are included in this Authorization Boundary if the CSP manages/secures the operating system and platform applications.
SaaS	• May build on the devices, platforms, applications, or constructs used in IaaS and PaaS to encompass the final application that constitutes the CSP's service offering and everything that supports it. • Some, if not all, that are listed for IaaS and PaaS are included in this Authorization Boundary for SaaS.

2. **The Mission Owner's System/Application Authorization Boundary:** This boundary is addressed by the Mission Owner's ATO.
   - The Mission Owner's system/application inherits the CSO(s), residual risk, and security controls that the CSP implements for their organization.
   - The Mission Owner's ATO covers the inherited security controls along with the following based on service type:

Table 4-2: Mission Owner Boundary Based on Service Type

Service Type	Mission Owner Boundary
IaaS	• The Mission Owner operated/maintained system of virtual networks and VMs including their operating systems, applications, and associated data storage.
PaaS	• The portion of the system of virtual networks and VMs including their operating systems, platform applications, and associated data storage managed by the Mission Owner. • Application(s) implemented by the Mission Owner on top of the CSO.
SaaS	• The portion of the CSO managed by the Mission Owner (e.g., user accounts) along with the Mission Owner policies and procedures for using the CSO. • The Mission Owner's compliance with DOD security policies related to the use of the CSO and Cloud in general.
All Service Types	• Data-in-transit encryption methods used by the Mission Owner. • Any additional layers of access control implemented by the Mission Owner for access to the service for users and management. • Data at rest encryption implemented or managed by the customer. • Any other DOD requirements that must be met by the CSP's customer.

4.3.2 CSO Risk

The DOD PA provides a provisional or partial risk acceptance determination for the CSO against the appropriate DOD security requirements. The DOD PA assessment process assesses and highlights CSO risk based on its supported Impact Level. At Level 4 and above, the DOD PA evaluation process assesses the risk of permitting CSPs to connect to DOD networks.

4.3.3 Mission Risk

Mission refers to the information system and functions for which a DOD entity acquires or uses a CSO. This may include the direct use of an SaaS CSO in performing an IT-enabled mission or the instantiation of an IT system or application on an IaaS/PaaS CSO.

Any DOD or non-DOD CSO available for use across the DOD by multiple Mission Owners must have been issued a DOD PA by DISA. The mission risk will continue to be assessed and authorized by the Mission Owner's AO through the issuance of an ATO.

The Mission Owner's system/application/cloud use case must be issued an ATO by their Component's AO or a component-authorized subordinate AO. This mission system ATO requirement is applicable at all information Impact Levels and extends to:

- DOD CSP IaaS/PaaS CSOs where an ATO has been granted instead of a PA, since its ATO or PA only permits its connection to the DISN, and since such an ATO cannot address full mission system/application risk when built on the CSO.
- DOD CSP SaaS CSOs that only have a PA.

Note: A Mission Owner may use DOD CSP SaaS CSOs (that have an existing ATO) without needing to create a separate ATO.

A DOD PA is required when a Mission Owner uses a CSO that is provided by a third-party integration contractor or reseller of CSP CSOs (i.e., any CSO being integrated into a solution for use by DOD or resold to a DOD entity must have a DOD PA).

Mission owners categorize mission systems and/or applications in accordance with DODI 8510.01 defined processes. Mission owners then select CSOs from the DOD Cloud Service Catalog based on their security posture and risk tolerance of the Mission Owner and their AO. While CSOs will have been assessed and provisionally authorized for use, the Mission Owner must undergo the RMF process to obtain an ATO from their assigned AO.

The Mission Owner inherits compliance from the CSO for the security controls met and maintained by the CSP.

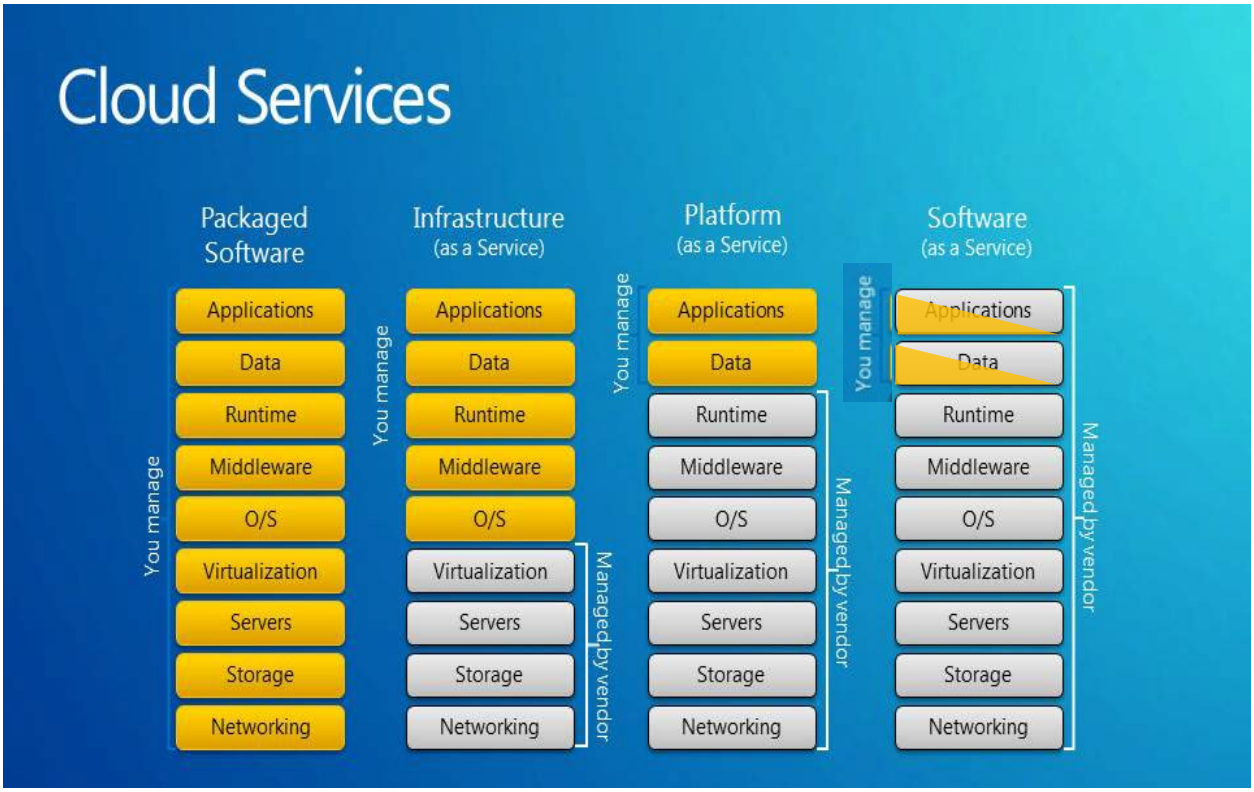
- A Mission Owner's system or application built on an IaaS or PaaS offering will be subject to meeting similar security controls within the system/application.
- Mission owners contracting for SaaS offerings inherit the bulk of compliance with the security controls from the CSO.
- Inheritance will vary between CSPs operating within a given service model and therefore must be evaluated separately.

Note: The number of controls increases with higher Impact Levels and additional overlay controls (e.g., privacy).

Figure 4-1 depicts the division of management, the responsibility shared between the CSP and Mission Owner, and the concept of inheritance.

Figure 4-1: Notional Division of Security Inheritance and Risk

(Graphic courtesy of Microsoft)



Mission owners and their AOs must review the FedRAMP and DOD PA artifacts to understand the risks the mission will inherit when using the selected CSO for the mission system/application. Mission owners may need to implement, or request that the CSP implement, compensating controls for any risk deemed unacceptable prior to obtaining an ATO. Additional compensating controls must be reflected in the Mission Owner's SLA/contract with the CSP.

4.4 Assessment Impact of Cloud Computing SRG Updates

The requirements in Cloud Computing SRG documents may change with new releases and updates of the documents. Changes to security requirements become effective immediately upon final publication. However:

- Any new CSP/CSO assessment starting 30 days after the release of a Cloud Computing SRG update will be assessed against the previous requirements.
- CSPs/CSOs that are in the process of being assessed against the requirements in the previous Cloud Computing SRG will proceed with the active assessment. Active assessment is defined as any assessment process in which the CSP/CSO has partnered with a federal agency (i.e., the Agency AO has submitted a formal In Process Request to the Project Management Office) or has contracted with a 3PAO for an assessment. However, the CSPs/CSOs must transition to compliance with the current Cloud Computing SRG update in coordination with their next FedRAMP/DOD annual assessment (i.e., one year from award of the PA).

- CSPs/CSOs currently in continuous monitoring under the previous Cloud Computing SRG will provide a Plan of Action and Milestones (POA&M) within 30 days. These CSPs/CSOs must comply with the current Cloud Computing SRG requirements as soon as possible but no later than their next FedRAMP/DOD annual assessment (i.e., transition is to occur as soon as practical but no longer than between six months and one year).
- Any existing IL5/NSS systems will have two years from publication date to update to NIST SP 800-53 Rev 5. They must submit a POA&M within 30 days outlining actions needed to comply with requirement to move to the High baseline requirement.

A DOD PA issued for a CSP that uses the previous Cloud Computing SRG and is based on FedRAMP Moderate Baseline (MBL) or High Baseline (HBL) remains in effect for the duration of the DOD PA (unless revoked), so long as compliance is achieved with the timelines described above. Due to the transition period, DOD mission systems leveraging a CSO may experience a period where risks based on the current Cloud Computing SRG security controls have not yet been assessed. Mission Owners and their AOs must review the controls to determine if the risk is acceptable until the CSP is required to comply or include the required compliance in the SLA/contract.

4.5 DOD PA in Relation to RFP Response and Contract Award; DFARS Interpretation

This section provides information about PAs and ATOs in relation to contract awards. The following points in no way alter any contract clauses that are currently defined in the Defense Federal Acquisition Regulation Supplement (DFARS) or that may be defined in the future. They are intended to provide additional clarity primarily regarding on-premises CSOs.

This topic must be addressed from two viewpoints. These are:

- When the commercial CSO infrastructure is off-premises (where it is typically already in existence).
- When the CSO infrastructure is contracted to be on-premises either physically or virtually (where it typically will need to be built using dedicated hardware).

Off-Premises Commercial Service: In accordance with DFARS SUBPART 239.76—CLOUD COMPUTING, 239.7602-1 (b)(1), a CSP must have a DOD PA at the appropriate information Impact Level before contract award. The CSP/CSO must have a DOD PA before responding to a DOD cloud services RFP or show evidence that the CSO can achieve a DOD PA before contract award.

This extends to integrators and resellers of CSP CSOs responding to RFPs (i.e., any CSO being integrated into a solution for use by DOD or resold to a DOD entity must have a DOD PA at the appropriate Impact Level).

DFARS 239.7602-1 (b)(2) provides two exceptions:

- The requirement for a provisional authorization is waived by the DOD CIO; or

- The cloud computing service requirement is for a private, **on-premises** version that will be provided from U.S. government facilities. Under this circumstance, the cloud service provider must obtain a provisional authorization prior to operational use.

If a Mission Owner leverages a commercial off-premises CSO and its PA, the Mission Owner's AO will provide the ATO for their use of the CSO to meet DOD RMF policy.

On-Premises (Physically or Virtually): The general DFARS rule applies to on-premises CSOs in that it is beneficial to DOD that the commercial instantiation of the CSP's CSO has been assessed and awarded a DOD PA. This proves the commercial service and infrastructure is capable of hosting DOD information and systems at the appropriate information Impact Level. However, this PA is not directly useable for a separate on-premises instantiation of the CSO.

An on-premises CSO is DOD private, which will be connected to a DISN service (i.e., NIPRNet or SIPRNet). The CSO must have a DOD Interim Authority to Operate (IATT), conditional ATO, or PA to connect to the network for testing and must also possess a DOD ATO (with or without conditions) before going into production following normal DOD policy.

A previous DOD PA for the off-premises commercial instantiation will only inform the assessments for the on-premises IATT and ATO. Certain portions of the previous PA assessment will have to be reassessed due to the new infrastructure and different location(s). Some security control compliance will be inherited from the DOD and the specific facility where the CSO infrastructure is located rather than the commercial facility. In a virtually on-premises scenario, the instantiation might inherit some security control compliance from the DOD PA for the commercial service and the commercial data centers where it is hosted, providing the private instantiation is hosted in the same data center(s) as were reviewed for the PA.

As stated above, DFARS provides an exception to the general rule that a CSP/CSO must have a DOD PA before award. A contract may be awarded for a private on-premises CSO that will be provided from U.S. government facilities. The clause also states that the CSO must obtain a PA prior to operational use. Alternately, on-premises DOD systems, including CSOs, may require an ATO before operational use. This ATO may be used in lieu of a PA or to generate a PA that would be leveraged by Mission Owners and their AOs.

While an RFP may require a CSO to meet all the requirements outlined in the DOD Cloud Service Provider SRG for Impact Level 2/4/5/6, this excludes on-premises CSOs regarding a PA before award. Furthermore, unless a CSP already offers an Impact Level 6 CSO that has an Impact Level 6 PA, it is impossible to obtain a DOD Impact Level 6 PA before a contract award. This is because a CSP cannot obtain an Impact Level 6 PA unless a contract is in place that generates a DD-254, thus allowing a DCSA facility clearance to be obtained for the facilities housing the CSO. Unless a CSP has other contracts whereby their CSO is already in a cleared facility, an Impact Level 6 PA cannot be granted.

4.6 Assessing Managed IT Cloud Service Vs. Cloud Service

For a Managed IT Cloud Service, the customer dictates the technology and the operational procedures. However, for a Cloud Service, the CSP dictates the technology and the operational procedures.

An on-premises, DOD private CSO operated by a contractor (the original CSP or other organization) can be a Managed IT Cloud Service. This happens when DOD contracts for a "copy" or "version" of a CSP's commercial cloud service to be built on DOD premises (virtually or physically) and operated/managed as a private CSO.

DOD private Managed IT Services are assessed using DOD security requirements and RMF policy but are not subject to DOD policy addressing commercial cloud services. However, Managed IT Cloud Service assessments include requirements in this Cloud Service Provider SRG as well as DOD and RMF security requirements.

4.7 Considerations for Impact Level 4/5 DOD PA Award

The following is a list of considerations and/or requirements that must be assessed or reviewed in addition to the security control assessments for AO acceptance before an Impact Level 4/5/6 DOD PA is awarded. The listing may not be all-inclusive.

- How support for DOD PKI authentication by DOD privileged and nonprivileged users is implemented. This includes the processes and protocols used along with their implementation.
- How support for DOD IP addressing will be implemented.
- CSP data center locations hosting the CSO for which the PA is to be awarded.

  CSO management/monitoring plane (and/or specific devices/systems) and its integration with the CSP's corporate network or the general commercial CSO management plane. No specifics are provided regarding this consideration at this time; however, refer to the next item for related concerns.
- CSP personnel managing and/or monitoring the CSO infrastructure. This is primarily related to U.S. Persons constraints. Refer to Section 5.5.2, CSP Personnel Requirements.
- The availability of a private connection capability between the off-premises CSP's/CSO's network and DOD networks in support of connections through the Boundary Cloud Access Point (BCAP) and meet-me points.
- Reliance of the CSO or user experience on internet-based capabilities such as the public DNS or content delivery networks. All such capabilities must be available via the CSO infrastructure and the connections to it via the DISN BCAPs. The CSO must be able to function if DOD limits access to or disconnects from the internet in times of conflict or when the DISN/DODIN is being attacked. No specific requirements other than those noted here are provided.
- Reliance on internet access to reach the CSO management/service-ordering portal or API endpoints from NIPRNet or from within the CSO. All such access must be via the CAP if from the NIPRNet or must remain on the CSP's/CSO's network if from within the CSO. These requirements must be minimally configurable if not inherent. No specific requirements other than those noted here are provided.
- The protections in place in the CSP's network and CSO to prevent any internet connection to the CSP's/CSO's network and CSO from becoming a back door to the NIPRNet via the private connection through the BCAP.

- The robustness of the CSP's required boundary protection (defense-in-depth security/protective measures) implemented between the internet and the CSO for its protection from internet-based threats. This protection is expected to be different depending on whether the CSO is I/PaaS or P/SaaS and whether the Mission Owner has control over their portion of the CSO.
- All other requirements as defined in the rest of this SRG.
- Other considerations as realized while assessing the CSO or because of lessons learned.

5. SECURITY REQUIREMENTS

This section of the Cloud Service Provider SRG defines the security requirements for DOD's use of cloud computing. It focuses on security requirements for assessing CSOs for the award of a DOD PA and inclusion in the DOD Cloud Service Catalog while hosting DOD missions. Mission Owner requirements are primarily addressed using the Cloud Computing Mission Owner SRG; however, some Mission Owner requirements and controls remain here.

Appendix D provides mandatory RMF values for DOD parameters in addition to FedRAMP and additional controls.

All CSP and CSO requirements in this Cloud Service Provider SRG apply to all CSPs and CSOs offered to or contracted by the DOD. DOD recognizes that CSOs may be offered by a CSP or an Integrator as the prime contractor on a DOD contract. DOD also recognizes that prime contractors may subcontract for multiple CSOs to meet contract capabilities requirements and may subcontract systems maintenance. Therefore, all requirements in this Cloud Service Provider SRG apply to all CSOs provided by prime contractors and their subcontractors, including systems maintenance contractors who may have access to CSP customer information or the capability to affect the security of the CSO. This flow down to subcontractors is also covered in cloud and contractor associated DFARS clauses.

5.1 DOD Policy Regarding Security Controls

NIST SP 800-53 and FedRAMP baselines are the foundation for the security controls selected for cloud-based systems. However, additional security controls and/or overlays will be required depending on the mission and data to be processed/stored. Refer to NIST SP 800-53 and CNSSI-1253.

5.1.1 DOD FedRAMP+ Security Controls

DOD FedRAMP+ refers to a tailored baseline of security controls developed for each DOD information Impact Level, except for Impact Level 2. These baselines include but are not limited to the FedRAMP Moderate or High baselines. The FedRAMP+ security controls include NIST 800-53 security controls, parameter values, and enhancements not included in the FedRAMP baselines. The FedRAMP+ security controls were selected primarily because the DOD, unlike the rest of the federal government, must categorize its systems in accordance with CNSSI 1253, use its baselines, and then tailor them as needed.

The CNSSI 1253 baselines used in support of DOD PAs are based on Moderate or High Confidentiality, Integrity, and Availability. The Mission Owner must address availability in the contract/SLA.

5.1.2 Parameter Values for Security Controls and Enhancements

Both FedRAMP and the DOD have defined minimum requirements in security controls and enhancement parameters. However, in some circumstances, the specifics of the implementation are left to the CSP and assessed as to whether the implementation is appropriate for the CSO and

government. For controls required by FedRAMP and the DOD, the parameter values are defined in Appendix D.

5.1.3 National Security Systems (NSS)

Impact Levels 5/6 are designed to accommodate NSS. CNSSI 1253 NSS-specific security controls must be included for any NSS in the cloud. Thus, unclassified NSS must be instantiated at Impact Level 5. This does not preclude an unclassified non-NSS from operating at Impact Level 5 if the mission/information owner requires the added security.

The NSS-specific security controls of a CSP's CSO must be assessed for any Impact Level containing NSS information for a DOD PA. For all CSOs, only some of these security controls maybe applicable to the CSP, with the balance fulfilled by the Mission Owner.

5.1.3.1 NSS Level 6 Classified Overlay Applicability

Impact Level 6 is for classified systems that are National Security Systems. All CSOs are subject to the CNSSI 1253 Classified Information Overlay in addition to FedRAMP and FedRAMP+. For the Classified Information Overlay, refer to CNSSI 1253. This overlay imposes additional security controls that must be assessed for a CSP's CSO Impact Level 6 PA. For all CSOs, only some of these security controls may be applicable to the CSP, with the balance fulfilled by the Mission Owner.

5.2 Data Ownership, Separation, and Protection

This section addresses legal requirements for the location of DOD information, who may have access to it in CSP facilities and CSOs, and protection.

5.2.1 Legal Jurisdiction and Location

This section addresses legal jurisdiction over information controls where DOD and U.S. government data can be processed/stored. This is nuanced by the information being on DOD premises.

To protect against seizure and improper use by non-U.S. persons and government entities, all data stored and processed for the DOD must reside in a facility under the exclusive legal jurisdiction of the United States. This may include DOD bases on foreign soil, depending on Status of Forces Agreements (SOFA). CSPs will maintain all government data that is not physically located on DOD premises within the 50 States, the District of Columbia, and outlying areas of the U.S. (as defined at FAR 2.101), unless otherwise authorized by the responsible AO as described in DODI 8510.01. The contracting officer will provide written notification to the contractor when the contractor is permitted to maintain government data at a location outside the 50 states, the District of Columbia, and outlying areas of the United States (DFARS SUBPART 239.7602-2).

CSPs will provide the Agency with a list of the physical locations where the data could be stored at any given time and update that list as new physical locations are added. The Mission Owner and/or

Contracting Officer must review CSP Terms and Conditions to ensure data stored and processed in U.S. data centers does not fall under the legal jurisdiction of another country.

On-premises CSOs implemented by a DOD or non-DOD CSP, which uses a hybrid model employing off-premises CSPs and CSOs to augment the on-premises CSO or by virtually extending the DOD fence line (DISN boundary), must also meet the location requirements stated here.

An exception is made for content delivery networks (CDN) in which non-sensitive DOD data may be cached anywhere in the world. However, when sensitive information is requested through a CDN, the request must be sent back to its storage facility under U.S. jurisdiction for retrieval.

Corresponding Security Controls: SA-9(5).

5.2.1.1 DOD Off-Premises vs. On-Premises vs. Virtually On-Premises

DOD on-premises versus off-premises relates to the physical or virtual location of a facility or IT infrastructure.

DOD Off-Premises: A facility (building/container) or IT infrastructure is off-premises if it is NOT physically or virtually on DOD-owned or -controlled property (i.e., on-premises). Refer to DOD On-Premises and DOD Virtually On-Premises below and their definitions for additional details.

DOD On-Premises: A facility (building/container) or IT infrastructure is on-premises if it is physically on DOD-owned or -controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DOD installation (i.e., Base, Camp, Post, or Station [B/C/P/S] or leased commercial space) under the direct control of DOD personnel and DOD security policies.

DOD On-Premises includes DOD data centers and other facilities located on a DOD B/C/P/S or in a commercial or other government facility (or portions thereof) under the direct control of DOD personnel and DOD security policies. A commercial facility, in this sense, means a building or space leased and controlled by DOD. Such facilities are within the protected perimeter or "fence line" of a DOD-controlled installation or property. Physical facilities may be permanent buildings or portable structures such as transit/shipping containers. An example of the latter might be a shipping container housing a commercial CSP's infrastructure located adjacent to a Core Data Center (CDC) and connected to its network as if it were inside the building.

DOD CSPs will, and commercial CSPs may (under DOD contract), instantiate their CSO architecture on DOD premises (DOD on-premises). Interconnection with DOD networks will be interoperable in accordance with engineering requirements that meet cybersecurity guidance and controls. Such implementations will be considered DOD Private.

DOD Virtually On-Premises: A DOD Private IT and/or CSO infrastructure located in a physically off-premises location (facility), such as a federal government or commercial data center (i.e., facilities under the direct control of non-DOD personnel using non-DOD security policies), may be considered Virtually On-Premises under specific conditions as listed below. These conditions apply certain physical security controls and extend the DISN accreditation boundary. This construct virtually extends the DOD-protected perimeter or "fence line" around the infrastructure. It also places the IT/CSO infrastructure and its management plane in one or more

DISN enclaves, thus enabling alternative approaches for boundary protection, such as using CSO-provided infrastructure in lieu of a dedicated DOD ICAP/BCAP.

An IT/CSO infrastructure may be considered Virtually On-Premises under the following conditions:

Note: Items with an * are related controls that are not on the FedRAMP Moderate baseline.

- The CSO infrastructure is DOD Private/Community and its infrastructure, devices, monitoring/support infrastructure, and management plane are dedicated to it; physically separate from other infrastructure, devices, and network enclaves in the data center.
- DISN Transport is extended to the CSO's network enclave(s) supporting the CSO infrastructure, CSO monitoring/support infrastructure, and CSO management plane.
- Enclave/data center boundary protections are implemented to protect the CSO operational enclave(s) (which may include the CSO monitoring/support infrastructure) in accordance with DISN enclave boundary or CDC protection requirements.
- The CSO infrastructure is managed from one or more enclave(s) dedicated to managing the CSO. This can be done using dedicated workstations in the enclave or remotely using dedicated virtual desktop infrastructure (VDI).
- Enclave boundary protections are implemented to protect the dedicated CSO management/monitoring/support enclave(s) in accordance with DISN enclave boundary protection requirements.
- The CSO infrastructure is housed in a physically separate/protected space such as a cage or room (or minimally one or more locked cabinets with closed nonremovable sides closing the DOD space) within the commercial data center used to house the DISN network device(s) and CSO infrastructure. Related security controls: PE-3, PE-3(1)*, PE-3 (4)*, PE-4.
- This physically separate space is minimally protected as follows:
  - Physical access to the data center complies with all required physical and maintenance personnel access security controls in the FedRAMP Moderate or High Baseline as appropriate. This includes but is not limited to personnel role-based access control, access auditing, visitor access control and escorting as needed, etc. Related security controls: MA-5, MA-5(1), PE-2, PE-2 (3)*, PE-3, PE-3(1)*, PE-6, PE-6(1). PE-6(4)*, PE-8.
  - Physical access to the DOD space complies with all required physical and maintenance personnel access security controls in the FedRAMP Moderate or High Baseline as appropriate (as described above for the data center) and/or appropriate CNSSI 1253 baselines. Additional or alternate physical security and personnel controls may be required for facilities housing classified systems.
  - Personnel access is controlled by an automated entry access control system that is token and/or biometric based. This system may be under DOD control or the control of the facility owner but must limit access to only authorized individuals, must log/audit all accesses, including the identities of the personnel accessing and departing, and must provide and log alerts for unauthorized accesses and failed attempts. Related security controls: PE-6, PE-6(1) and PE-6(4)*.
  - The facility owner externally monitors access to the physical space using video cameras and a Physical Intrusion Detection System (PIDS) (i.e., intrusion alarm system). Related security controls: PE-6, PE-6(1), PE-6(3)*, and PE-6(4)*.

- It is highly recommended that the internal space be monitored by an automated motion-activated PIDS and video cameras operated by DOD. In this manner, DOD can monitor all physical activities within the space, authorized or unauthorized. Related security controls: PE-6, PE-6(1), PE-6(2)*, PE-6(3)*, and PE-6(4)*.

5.2.2 Impact Level Separation Requirements

The risks and legal considerations of using virtualization technologies further restrict the types of tenants that can obtain cloud services from a virtualized environment on the same physical infrastructure and the types of cloud deployment models (i.e., public, private, community, and hybrid) in which the various types of DOD information may be processed or stored.

While shared cloud environments provide significant opportunities for DOD entities, they also present unique risks to DOD data and systems that must be addressed. These risks include exploitation of vulnerabilities in virtualization technologies, interfaces to external systems, APIs, and management systems. These have the potential for providing backdoor connections and CSP privileged user access to customers' systems and data. While proper configuration of the virtual and physical environment can mitigate many of these threats, the residual risk may or may not be acceptable to DOD. Legal concerns such as e-discovery and law enforcement seizure of nongovernment CSP customer/tenant's data pose a threat to DOD data if it is in the same storage media. Due to these concerns, DOD is taking a cautious approach regarding Impact Level 5 information.

Infrastructure (as related to cloud services) is the physical hardware (i.e., servers and storage) and the network interconnecting the hardware that supports the cloud service and its virtualization technology (if used). This includes the systems and networks used by the CSP to manage the infrastructure. While the physical space where this infrastructure is housed is part of the CSP's infrastructure, this is not a factor in DOD's separation restrictions except at Impact Level 6.

Dedicated infrastructure refers to the cloud service infrastructure being dedicated to serving a single customer organization or a specific group of customer organizations (a community). A private cloud service implements dedicated infrastructure to serve one customer organization or community. This SRG considers DOD as the organization that consists of all DOD components. This SRG restricts private cloud for DOD as meaning dedicated infrastructure that serves multiple DOD users and tenants. A DOD private cloud or CSO may be multitenant, serving all or some DOD components (DOD community), or may be single tenant, serving a single mission. A community cloud service implements dedicated infrastructure to serve a specific group or class of customer organizations. Because the definition of DOD private could also be considered a DOD community cloud, this SRG will use the term DOD private/community. This SRG will also use the term federal government community, meaning dedicated multitenant infrastructure that serves DOD components as well as other federal government agencies.

Corresponding Security Controls: SC-4.

5.2.2.1 Impact Level 2 Location and Separation Requirements

Impact Level 2 cloud services can be offered on any of the four deployment models. Information that may be processed and stored at Impact Levels 2 can be processed on-premises or off-premises; the physical location of the information is restricted.

For an Impact Level 2 PA, DOD currently is accepting the risk that this is adequately covered by a FedRAMP Moderate PA, and the requirement will not be additionally assessed for an Impact Level 2 PA.

5.2.2.2 Impact Level 4 Location and Separation Requirements

Impact Level 4 cloud services can be offered on any of the four deployment models. Information that may be processed and stored at Impact 4 can be processed on-premises or off-premises if the physical location of the information is restricted.

For an Impact Level 4 PA, the CSP must provide evidence of strong virtual separation controls and monitoring to support "search and seizure" requests for non-DOD information and data without the release of DOD information and data and vice versa. Additionally, the strong virtual separation controls must prevent/mitigate/eliminate the potential vulnerability whereby one CSP customer using the same physical hardware as another CSP customer can gain access to the other's information/data, virtual network, or virtual machines. Monitoring must detect such unauthorized accesses and/or attempts to enable incident response.

5.2.2.3 Impact Level 5 Location and Separation Requirements

Impact Level 5 information must be processed in a cloud community, on-premises or off-premises in any cloud deployment model that restricts the physical location of the information.

The following applies:

- IL5/NSS cloud environments must either be physically separated from all non-federal tenant systems and infrastructures or must have the cryptographic (virtual) separation validated or approved by NSA. CSP is responsible for accomplishing all coordination with NSA. Refer to Section 5.2.4.4, Requesting an NSA Encryption and KMS Evaluation.

  Note: "Federal information system" is an information system that is used or operated by an executive agency, a contractor of an executive agency, or another organization on behalf of an executive agency. A system that does not meet such criteria is a nonfederal system (NIST SP 800-171 rev 2 and 40 USC 11331, Subchapter III, sec 11331, page 209, para g).
- All IL5/NSS data must remain under U.S. jurisdiction or in U.S. Territories or geographic locations where there is U.S. jurisdiction.

5.2.2.4 Impact Level 6 Location and Separation Requirements

Impact Level 6 is reserved for the storage and processing of information classified up to SECRET. Information that must be processed and stored at Impact Level 6 can only be processed in a DOD private/community or federal government community cloud, on-premises or off-premises in any cloud deployment model that restricts the physical location of the information.

The following applies:

- Impact Level 6 information up to the SECRET level must be stored and processed in a dedicated cloud infrastructure located in facilities approved for the processing of classified information, rated at or above the highest level of classification of the information being stored and/or processed.
- Impact Level 6 CSO infrastructure is a SIPRNet enclave and as such will be a closed self-contained environment for the CSO processing, storage, and management planes only connected to SIPRNet.
- Each deployment model may support multiple SECRET missions from multiple customer organizations.
- Virtual/logical separation between DOD and federal government tenants/SECRET missions is sufficient.
- Virtual/logical separation between tenant/mission systems is minimally required.
- Physical separation from non-DOD/non-federal government tenants (i.e., public, local/state government tenants) is required.

5.2.2.5 Separation in Support of Law Enforcement and Criminal Investigation and E-Discovery

Under federal law, the federal government reserves the right for law enforcement officials to perform criminal investigations of federal government employees and elected officials, as well as anyone with access to federal government information, for misconduct, misuse of such data, or incident investigation. Such criminal investigations may include a need for e-discovery on federal government information to collect digital evidence. Therefore, the CSP must be able to segregate federal government information from non-federal government information within the CSO.

The granularity of separation must be at the federal government Mission Owner level. The CSP must also ensure this segregation requirement flows down to all CSP/Integrator subcontracted CSP/CSOs. The CSP and subcontractors must then be capable, upon request of the contracting officer(s) or in response to a subpoena, of isolating one or more federal government Mission Owner's data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space or via secure remote connection with access limited to authorized government personnel identified by the contracting officer, and without the CSP's involvement, or provide a forensic digital image of the requested federal government information.

5.2.3 CSP Use of DOD Data

All DOD information/data placed or created by DOD users in a CSP's CSO is owned by the DOD, the Mission Owner, and/or their Information Owner unless otherwise stipulated in the CSP's contract with the DOD. The CSP has no rights to the DOD's information/data. DOD information/data includes logs and monitoring data created within and by a Mission Owner's system/application implemented in IaaS/PaaS CSOs as well as logs created for and provided to the Mission Owner related to their use and management of the CSO. DOD also maintains ownership of all information/data created by the CSP/CSO for DOD if such activities are part of the contract. CSPs seeking a DOD PA must agree that DOD remains the owner of all DOD data in a CSO.

CSPs are prohibited from using DOD data in any way other than that required to provide contracted services to DOD (e.g., customer access/usage logs used for billing) This means the CSP may not "data mine" DOD email, files, information in databases, or communications for any purpose other than that stipulated in the contract.

The CSP maintains ownership of all logs and monitoring data created within the CSO related to the Mission Owner's use and management of the CSO. This includes logs related to customer access and usage for billing, data for CSO capacity planning, and monitoring data related to malicious activities or CSO health. This also includes all audit content specified by the AU-2 security control for the time specified by AU-11. While the CSP retains ownership of this information, some or all must be shared with the Mission Owner for the purposes of planning, forensics, billing validation, retention, etc. The ownership of the copies of this information shared with the DOD/Mission Owner is maintained by the DOD/Mission Owner.

Additionally, all DOD information/data and CSP information/data shared with the Mission Owner must be made available for offboarding and backup.

Related Security Controls: AC-23.

5.2.4 Data Protection

5.2.4.1 Encryption of Data-at-Rest in Commercial Cloud Storage

Mission systems at all Impact Levels must have the capability for DOD data to be encrypted at rest with exclusive DOD control of encryption keys and key management. Some CSOs may facilitate this by providing a hardware security module (HSM) or offering customer-dedicated HSM devices as a service. CSOs that do not provide such a capability may require mission owners to use encryption hardware/software on the DISN or a cloud encryption service that provides DOD control of keys and key management. Some CSOs may offer a key management system (KMS) service that can suffice for management of customer keys by the customer while preventing CSP access to the keys. It is recommended that such CSP KMS services be evaluated by NSA.

Data-at-rest (DAR) encryption with customer-controlled keys and key management protects the DOD data stored in CSOs with the following benefits:

- Maintains the integrity of publicly released information and websites at Level 2 where confidentiality is not an issue.
- Maintains the confidentiality and integrity of CUI at Levels 4 and 5 with the following benefits:
  - Limits the insider threat vector of unauthorized access by CSP personnel by increasing the work necessary to compromise/access unencrypted DOD data.
  - Limits the external threat vector of unauthorized access by hackers by increasing the work necessary to compromise/access unencrypted DOD data.
  - Enables high-assurance data destruction for CSP offboarding through cryptographic erasure and file deletion without the involvement or cooperation of a CSP.

- Enables high-assurance data spill remediation through cryptographic erasure and file deletion without the involvement or cooperation of a CSP.
- Refer to Section 5.2.4.2, Cryptographic Erase, for additional information.

Note: Mission owners and their AOs should consider the benefits of DAR encryption for data destruction and/or spill remediation at Level 2 in addition to the benefit of maintaining information integrity.

For all information Impact Levels:

- Encrypt all DAR stored in:
  - Virtual machine virtual hard drives.
  - Mass storage facilities/services whether at the block or file level.
  - Database records (whether PaaS or SaaS where the Mission Owner does not have sole control over the database and database management system).
- Use FIPS 140-2 or FIPS 140-3 validated cryptography modules (minimally Level 1) operated in FIPS Mode in accordance with federal government policy/standards for the protection of all CUI.
  - Cryptography modules include cryptographic algorithm, RNG, KMI, HASH, etc. (all approved functions).
- The CSP customer/Mission Owner maintains control of the keys from creation through storage and use to destruction.
  - Implement hardware security modules or key management servers as needed to store, generate, and manage keys within the DISN; or
  - Order a CSP service that provides a dedicated hardware security module that is managed solely by the customer/Mission Owner; or
  - Order a CSP key management service that has been evaluated by NSA.

For cloud applications where encrypting DAR with DOD key control is not possible, Mission Owners must perform a risk analysis with relevant data owners before transferring data into a CSO. This analysis must consider that no high-assurance method may be available to remediate data spills or ensure destruction of data at the application's end of life and CSO offboarding. Mission Owner AOs are responsible for accepting these risks.

Note: CSP CSO DAR encryption capabilities and the ability to support the Mission Owner's DAR encryption requirements will be assessed and documented toward the award of their DOD PA.

Corresponding Security Controls: SC-28, SC-28(1).

5.2.4.2 Cryptographic Erase

Cryptographic erase is described in NIST SP 800-88 Rev 1:

> "Cryptographic Erase is an emerging sanitization technique that can be used in some situations when data is encrypted as it is stored on media. With CE, media sanitization is performed by sanitizing the cryptographic keys used to encrypt the data, as opposed to

sanitizing the storage locations on media containing the encrypted data itself. CE techniques are typically capable of sanitizing media very quickly and could support partial sanitization, a technique where a subset of storage media is sanitization. Partial sanitization, sometimes referred to as selective sanitization, has potential applications in cloud computing."

While much of the cryptographic erase guidance in NIST SP 800-88 is related to self-encrypting devices, this section expands on NIST's acknowledgement that cryptographic erase has applicability in cloud computing.

DAR encryption, coupled with exclusive customer control of cryptographic key management, provides DOD the ability to cryptographically erase data at rest without CSP assistance or cooperation. This capability, coupled with standard CSP-provided data deletion, offers the benefits described for DAR encryption in Section 5.2.4.1 above.

Data deletion refers to normal file or data record deletion methods used in file systems and databases. Deletion before or after cryptographic erase will restore resources to the CSP and will permit for the eventual overwriting of the data under normal operations.

To support cryptographic erase and the benefits it provides, DAR encryption must be performed at an appropriate level of granularity. This means that one key should not be used to encrypt all or large chunks of mission owner data.

Related Security Controls: MP-6(3), MP-6(8).

5.2.4.3 Key Management Requirements

This section addresses key management security requirements used to protect information in a cloud. Cryptographic processes are properly separated if they do not intermingle customers' key material and if a vulnerability in a key-relevant process does not compromise the security of other customers' keys.

- Cryptographic algorithms and protocols used in the cloud-based KMS must be implemented according to applicable cryptographic standards.
  - Cloud-based KMS components must have been evaluated against and determined to comply with applicable National Information Assurance Partnership (NIAP) Protection Profiles.
  - Cryptographic software modules used in cloud-based KMS must have received FIPS 140-2 or FIPS 140-3 accreditation.
  - Cryptographic hardware security modules used in cloud-based KMS must have received FIPS 140-2 or FIPS 140-3 Level 3 accreditation.
- Cryptographic algorithms, protocols, and procedures used in cloud-based KMS must be developed and maintained in accordance with a secure software development lifecycle process.
- The CSP must ensure the Mission Owner has control of the keys used to protect that mission's information.
- The CSP must provide secure methods for managing access to a mission's keys and information.

- The CSP must securely delete a Mission Owner's keys on demand from the Mission Owner.
- The CSP must provide the Mission Owner with the ability to make keys unrecoverable when deleted. The Mission Owner must accept the risk that the keys will no longer be available. If the CSP makes deleted keys recoverable by default, the CSP must inform the Mission Owner how long a key will be in a recoverable state.
- The CSP must provide the customer with secure methods for importing keys into the cloud and for exporting keys from the cloud.
- The CSP must ensure cryptographic processes that handle customer keys are securely separated from other processes.
- The CSP must have processes in place to detect malicious administrators or other inside attacker activities.
- The CSP must have security procedures in place to prevent CSP and other unauthorized personnel from gaining access to customer keys.
    - The CSP must encrypt customer keys while they are at rest in the cloud.
    - The CSP must protect customer keys using secure channels when the keys are transmitted internal to the cloud system.
    - The CSP must minimize the exposure of customer keys while the keys are being actively used for cryptographic purposes.
        - The CSP must ensure only the cryptographic process that is required to use an unencrypted key will have access to the key.
        - The CSP must ensure that an unencrypted key is not stored in memory longer than necessary.
        - The CSP must ensure that an unencrypted key is securely deleted from memory and disk when no longer needed.

Related Security Controls: SC-12, SC-12(6).

5.2.4.4 Requesting an NSA Encryption and KMS Evaluation

CSPs wishing to offer this service must contact the DISA Cloud Support office. DISA will engage NSA, and NSA will then establish a contractual arrangement with the CSO to perform the risk assessment.

The DOD will enter a Customer Service Request Portal (CSRP) request to NSA, specifically requesting this type of evaluation in support of the DOD Cloud Computing SRG. The DOD will direct the request to the Office of the National Manager (ONM), who will task the appropriate NSA organizations in the Cybersecurity Directorate (C1 – Analysis and Mitigations and C2 – Encryption Production and Solutions) to perform the evaluation. The length of the evaluation will be no shorter than three months. After the evaluation is complete, C1 and Y2 will produce documentation about the evaluation and provide a risk recommendation.

NSA will evaluate a cloud-based KMS against the security requirements detailed in this document by performing the following activities:

- Engagements with the CSP to gain insight into details about the architecture and cryptographic services that are relevant and cannot be gained from public literature.

- Analysis of the cloud-based KMS or documentation from the vendor regarding detailed operation of these services.
- Security analysis of the web tier to assess security posture against web vulnerabilities, such as incorrectly implemented access controls, common web vulnerabilities, or other attacks that could be used to compromise an account, and enumeration of controls in place to defend against such attacks.
- Analysis of the cloud architecture to determine how vulnerabilities in the architecture could allow malicious actors to gain access to DOD data or keys.
- Confirmation that the cloud vendor has relevant government certifications, FIPS validations, and NIAP Protection Profiles.

Direct platform testing will be the preferred method for evaluating requirements, but vendor attestation will be acceptable when direct platform testing is not feasible. Methods used to evaluate each requirement will be documented and considered when developing a risk recommendation for the cloud-based KMS solution.

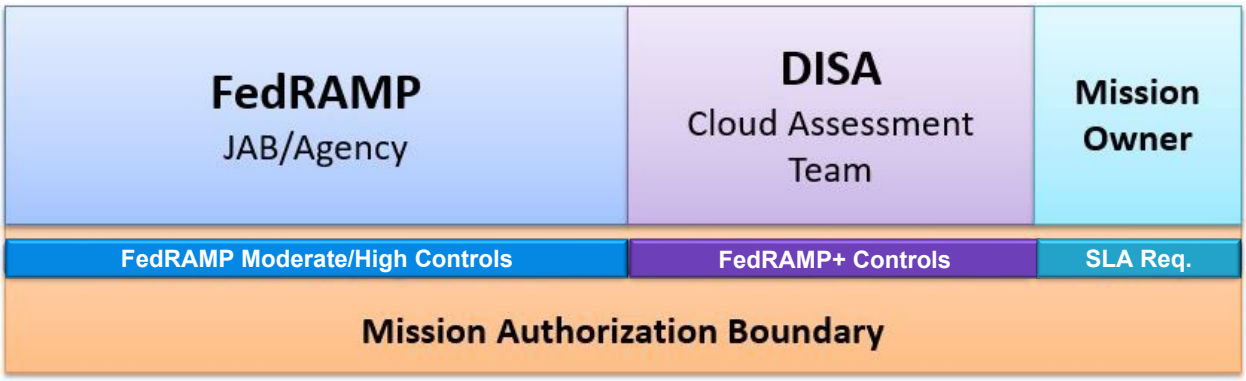
5.3 Ongoing Assessment

Both FedRAMP and DOD require an ongoing assessment and authorization capability for CSOs providing services to the DOD. This capability is built on the DOD RMF and the FedRAMP continuous monitoring strategy. These ongoing assessment processes, which are discussed in the following sections, include continuous monitoring and change control.

Ongoing assessment processes do not differ by Impact Level, although the artifacts produced as part of those processes may. (For example, Level 2 CSOs will have fewer controls to monitor than Level 4 CSOs.) These processes will differ, however, based on whether CSOs are part of the FedRAMP catalog or have a FedRAMP JAB PA. These differences are based on the division of responsibility over the set of security controls and the ability of DOD to access the artifacts produced as part of the FedRAMP processes.

Ongoing assessment responsibility mirrors the divided responsibilities and control inherent in cloud systems. FedRAMP's processes will be leveraged for all CSOs in the FedRAMP catalog. This process, however, covers only the portion of the system that is governed by the FedRAMP PA, such as the FedRAMP Moderate security controls. The DOD change control process will cover the portion of the system that is governed by the DOD PA, such as the FedRAMP+ security controls. The Mission Owner is responsible for ongoing assessment of controls levied by the Mission Owner, such as those that are specified in the SLA and do not fall under the FedRAMP or DOD PAs. This division of assessment responsibility is shown in Figure 5.1.

Figure 5-1: Ongoing Assessment Division of Responsibility



5.3.1 Continuous Monitoring

Once a DOD PA is granted, the CSP is expected to maintain the security posture of the CSO through continuous and periodic vulnerability scans, DOD annual assessments, incident management, and effective implementation of operational processes and procedures. Integral to this is periodic reporting to the appropriate AO. The continuous monitoring artifacts required to maintain a DOD PA are the same as those required by FedRAMP (annual assessments, monthly vulnerability scans, etc.). However, those artifacts must include additional information for FedRAMP+ controls and DOD requirements.

Continuous monitoring data flows will differ for CSPs depending on whether their CSOs have a FedRAMP JAB PA, a 3PAO-assessed non-DOD Federal Agency ATO, or DOD-assessed PA (as described in Section 4: Risk Assessments and Authorization). These data flows are reflected in Figures 5-2, 5-3, and 5-4, respectively.

In some cases, CSPs such as DOD Private CSOs or CSOs in the FedRAMP catalog with a non-DOD Agency ATO will provide continuous monitoring artifacts directly to DISA. In such cases, the CSP will use commercial standard formats (e.g., comma-separated values, XML) that enable DOD to automate the ingest of continuous monitoring data. For XML exchanges, National Information Exchange Model (NIEM)-based XML is the preferred format. Additional information regarding this format can be found at www.niem.gov.

All FedRAMP provisionally authorized CSP CSOs are required to have a 3PAO perform FedRAMP annual assessments to maintain their FedRAMP PA. DOD also requires annual assessments by a 3PAO or approved DOD SCA organization for the maintenance of their Level 4 and above DOD PA. CSOs in both the FedRAMP and DOD catalogs are expected to have a single annual assessment to cover this requirement for both FedRAMP and DOD. This means DOD will leverage and use the FedRAMP Continuous Monitoring (CONMON) process and artifacts to the greatest extent possible. CSOs in the FedRAMP catalog will follow the process described in the FedRAMP Continuous Monitoring Strategy Guide. DOD annual assessments will minimally include the set of controls listed in Appendix A of that document, as well as any other controls specified by the DISA AO. CSOs with a DOD PA that are not in the FedRAMP catalog will follow the DOD RMF process for continuous monitoring and associated assessments.

Corresponding Security Controls: CA-7.

5.3.1.1 Continuous Monitoring for CSOs in the FedRAMP Catalog with a DOD PA

The CSOs in the FedRAMP catalog that are eligible for DOD PAs include CSOs having a JAB PA (which is 3PAO assessed) or a 3PAO-assessed Federal Agency ATO. All reports required by the FedRAMP Continuous Monitoring Strategy Guide for these CSOs, including self-assessments, will be provided to the FedRAMP information system security officer (ISSO). These will be reviewed by the FedRAMP technical reviewers (which include DOD personnel) and approved by the JAB if necessary. DOD leverages the CSO's continuous monitoring artifacts and the work done by the FedRAMP technical reviewers.

Continuous monitoring requirements for DOD are the same as those for FedRAMP, except that all reports and artifacts for FedRAMP+ security controls will be provided directly to DISA AO representatives as the DOD single point of CSP contact for this information. DISA will share appropriate continuous monitoring information (FedRAMP and FedRAMP+) with Mission Owners, AOs, and cybersecurity service providers (CSSPs).

Mission Owners, their AOs, and the DISA AO will use the information to assess and authorize the CSO. The evaluations will inform decisions to continue the ATO for the Mission Owner's system and the PA for the CSP. The DISA AO will coordinate closely with Mission Owners if the withdrawal of a PA must be considered based on this requirement.

Figure 5-2 shows the normal flow of continuous monitoring information if the CSP has a FedRAMP JAB PA.

Figure 5-2: DOD Continuous Monitoring for CSOs with a FedRAMP JAB PA

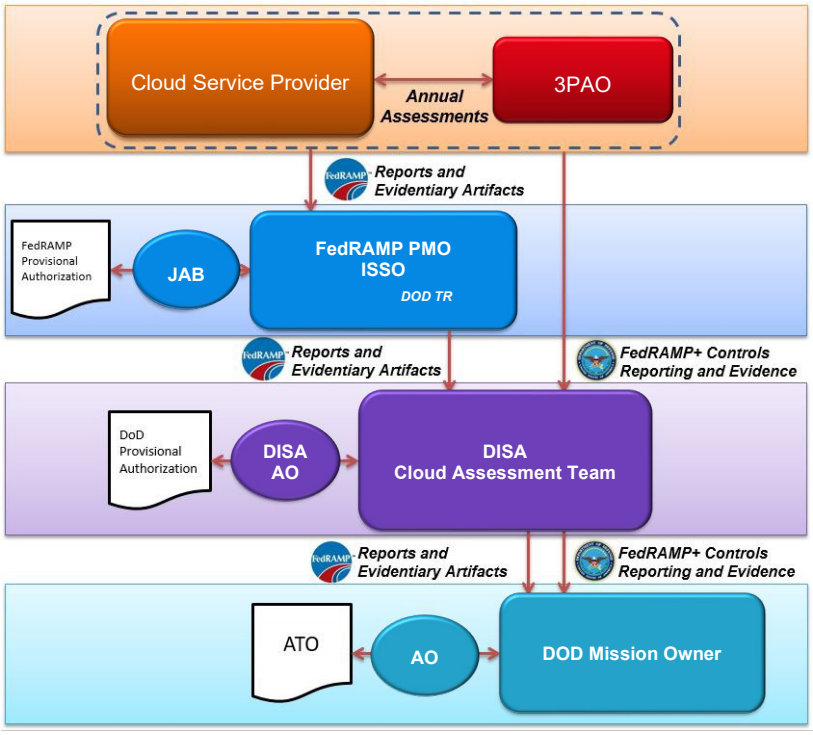
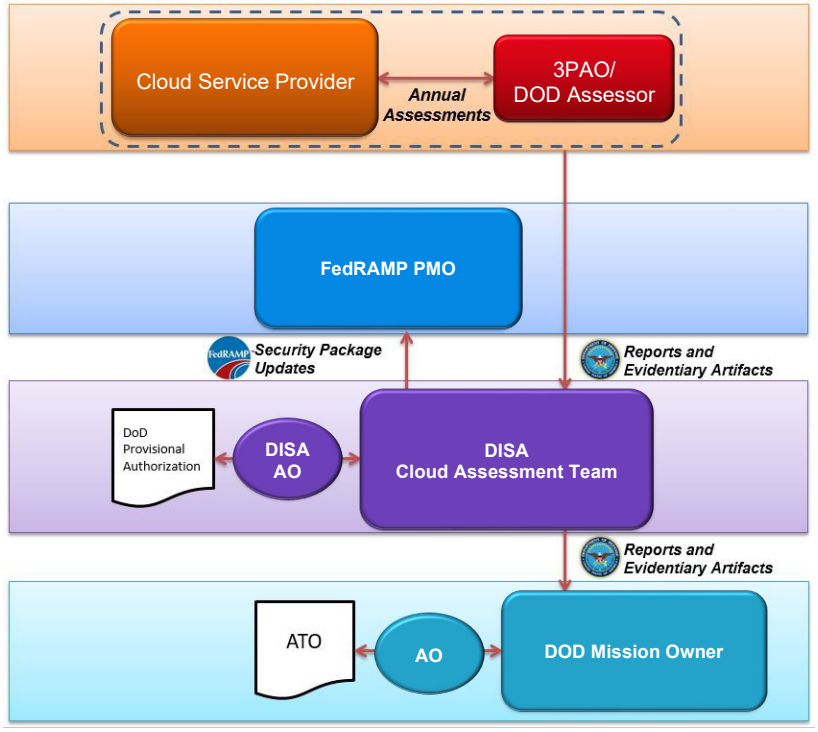


Figure 5-3 shows the flow of continuous monitoring information if the CSO has a 3PAO-assessed non-DOD Federal Agency ATO listed in the FedRAMP catalog. Because the FedRAMP JAB does not control the Agency ATO, information may not flow from the CSP to the FedRAMP PMO.

Figure 5-3: DOD Continuous Monitoring for FedRAMP CSOs with a 3PAO-Assessed Non-DOD Federal Agency ATO

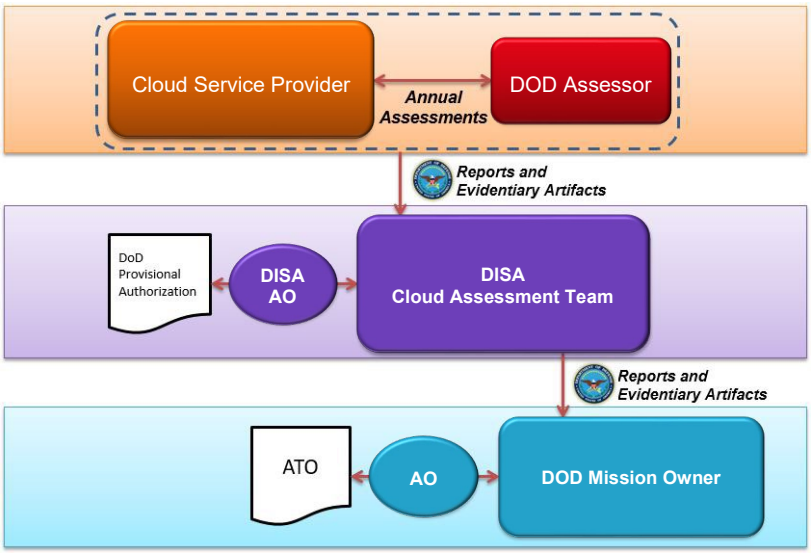


5.3.1.2 Continuous Monitoring for DOD-Assessed CSOs

Figure 5-4 shows the flow of continuous monitoring information for DOD private/community CSOs that have a DOD PA and ATO but are not in the FedRAMP catalog. Continuous monitoring will be directed by the DOD RMF, rather than the FedRAMP Continuous Monitoring Strategy Guide.

As part of the RMF authorization process, CSPs will create a continuous monitoring strategy that meets DOD requirements in the System Security Plan. The CSP will provide all reports and artifacts required by that continuous monitoring strategy to DISA. DISA will, in turn, disseminate those artifacts to all Mission Owners using that CSO, the DISA AO, and the CSSP.

Figure 5-4: DOD Continuous Monitoring for DOD-Assessed CSOs



5.3.2 Change Control

The DOD change control process for CSOs mirrors and leverages that of FedRAMP, with a focus on how changes affect the DOD PA and the security of hosted mission systems/applications and information.

CSPs must give DOD 30-day notice prior to significant changes. If a change that affects the risk posture of the system is made without approval, the DISA AO can revoke the DOD PA. As with continuous monitoring, the change control process will differ for CSPs depending on if they are in the FedRAMP catalog and if they have a DOD-assessed PA or ATO. Figure 5-5, Figure 5-6, and Figure 5-7 show these change control processes.

A significant change is likely to affect the security state of an information system.

Corresponding Security Controls: CM-3, CM-4, CA-6.

5.3.2.1 Change Control for CSOs in the FedRAMP Catalog with a DOD PA

The FedRAMP Continuous Monitoring Guide defines a significant change as a change to the scope of an approved PA or an impact to the authorization boundary of the CSO. The CSP will follow procedures defined in the FedRAMP Continuous Monitoring Strategy Guide by submitting a FedRAMP Significant Change Security Impact Analysis Form to the FedRAMP PMO.

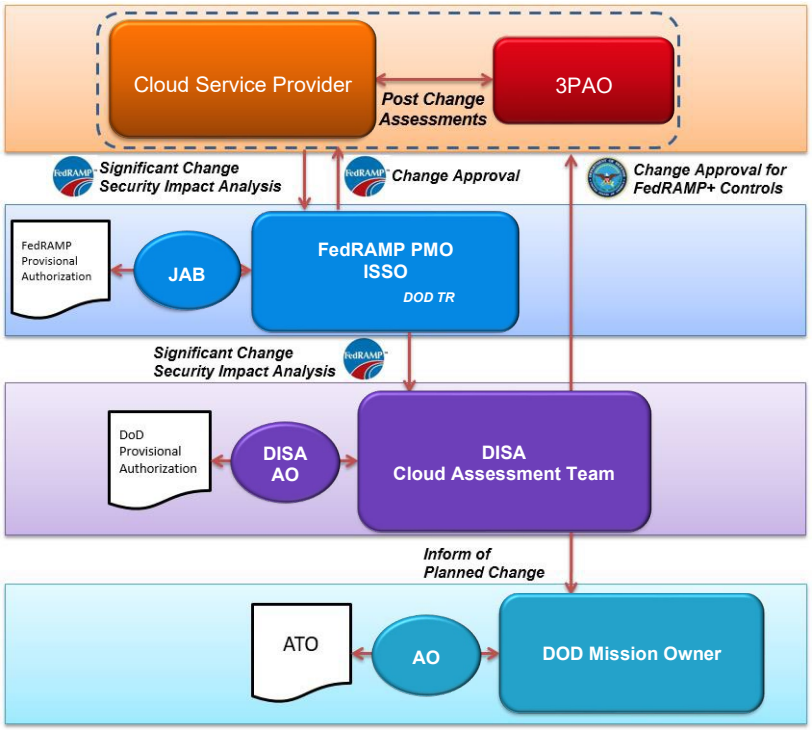
The review of the security implications of significant changes will be performed at multiple layers, as reflected in Figure 5-5. The FedRAMP ISSO and/or JAB technical representatives will review the planned change and then forward it to the JAB for approval. Simultaneously, the DOD JAB technical representative will notify DISA, which will in turn notify all Mission Owners using that CSO, the DISA AO, and CSSP. During FedRAMP ISSO review, the DOD JAB technical representative will collect comments from DOD stakeholders and inform the FedRAMP ISSO if planned changes will adversely affect the security of the information hosted by the CSO for DOD cloud customers.

DOD may communicate directly with the CSP and their 3PAO regarding change approval or concerns over the impact on DOD's FedRAMP+ security controls.

After a significant change is implemented, FedRAMP requires a security assessment by a 3PAO and the creation of a corresponding Security Assessment Report. CSPs must also include all FedRAMP+ security controls in post-change assessments to meet DOD requirements. DISA will notify affected Mission Owners of proposed significant changes and provide its assessment of the change within the scope of the CSO PA. Mission Owners are responsible for assessing the effects of proposed changes that fall within the scope of their SLAs.

Figure 5-5 shows the normal flow of significant change information if the CSP has a FedRAMP JAB PA.

Figure 5-5: DOD Change Control Process for CSPs CSOs with a FedRAMP JAB PA



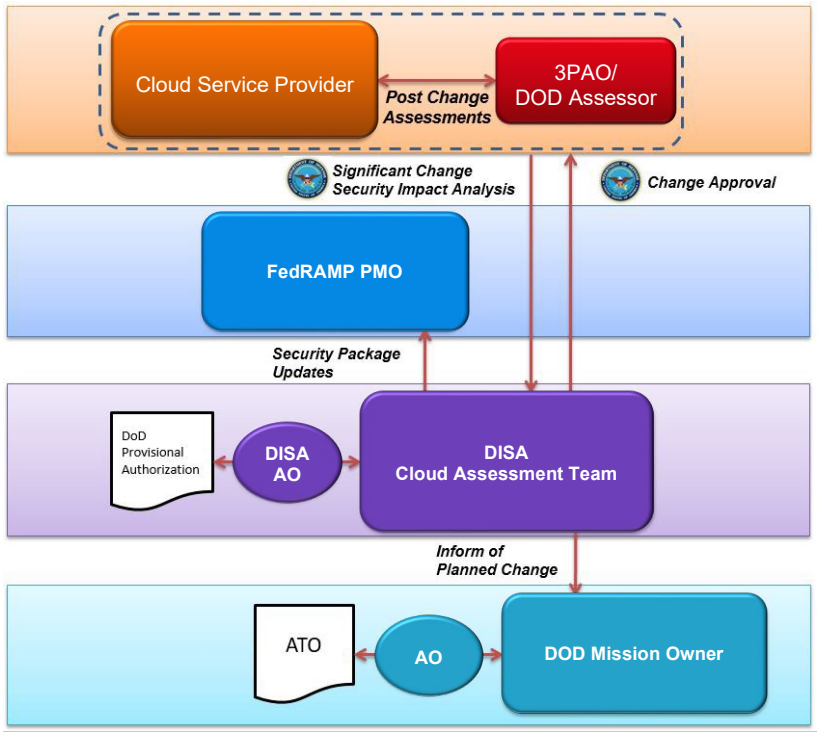
When a CSO with a DOD PA is included in the FedRAMP catalog but does not have a JAB PA, the CSP will notify DISA directly, in addition to any other required points of contact. (For example, a CSP with a non-DOD Agency ATO would notify both that agency and DISA). This is required because the FedRAMP JAB does not control the Agency ATO, and information may not flow from the CSP to the FedRAMP PMO and DISA.

DISA will notify all Mission Owners using that CSO, the DISA AO, and CSSP entities. The Security Impact Analysis must also cover the FedRAMP+ security controls. Once informed, DISA will review the proposed change to assess if it will, and ensure it will not, adversely affect the security of the DOD Information Network (DODIN) as a whole or the DISN with respect to the Impact Level at which it is authorized. Any updates to the FedRAMP Security Package will be forwarded to DISA.

As with FedRAMP, DOD requires a security assessment by a 3PAO after a significant change is implemented and the creation of a corresponding Security Assessment Report. CSPs must also include all FedRAMP+ security controls in post-change assessments to meet DOD requirements. DISA will notify affected Mission Owners of proposed significant changes and provide its assessment of the change within the scope of the CSO PA. Mission Owners are responsible for assessing the effects of proposed changes for effects that fall within the scope of their SLAs.

Figure 5-6 shows the normal flow of significant change information if the CSO has a 3PAO-assessed Non-DOD Federal Agency ATO listed in the FedRAMP catalog. Because the FedRAMP JAB does not control the Agency ATO, information from the CSP may not flow from the authorizing agency to the FedRAMP PMO. To avoid the possibility of DOD not being informed of potential changes, CSPs must send change requests to DISA in addition to the authorizing agency.

Figure 5-6: DOD Change Control Process for FedRAMP CSPs CSOs with a 3PAO-Assessed Federal Agency ATO

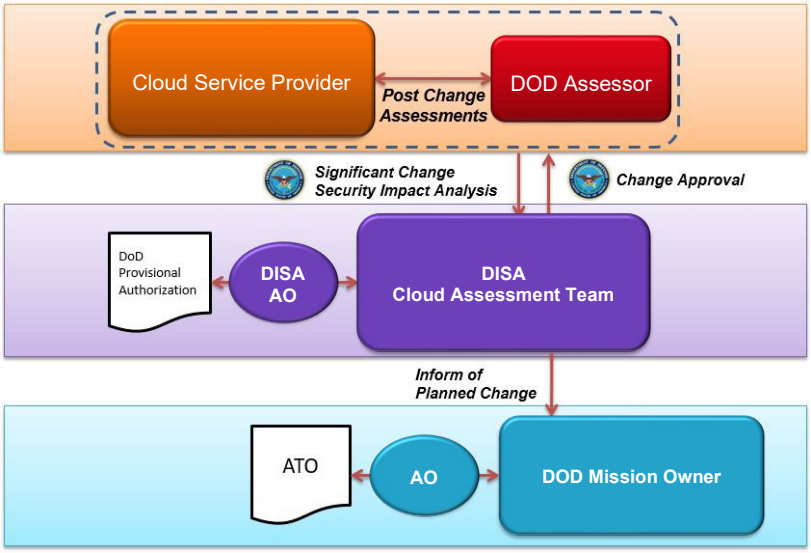


5.3.2.2 Change Control for DOD Assessed CSOs

Figure 5-7 shows the flow of significant change for non-FedRAMP CSOs having a DOD PA or ATO assessed by a DOD SCA organization and authorized by a DOD AO. The review of significant change information will be directed by the DOD RMF, rather than the FedRAMP change control process. CSPs will have similar responsibilities but will report directly to DISA. DISA will, in turn, disseminate those artifacts to all Mission Owners using that CSO, the DISA AO, and the CSSP entities. These entities will review the proposed change to ensure it will not adversely affect the security posture of the CSO with respect to its PA or ATO. The planned change will also be

reviewed by the Mission Owners using the CSO for any adverse impact regarding their specific use of the CSO.

Figure 5-7: DOD Change Control Process for DOD Self-Assessed CSPs/CSOs



5.3.3 Support for Financial Audits – SOC 1 Type II Reports

CSPs and their subcontractors provide annual System and Organization Control (SOC 1) Type II reports in support of DOD financial audits. DOD Mission Owners must add this requirement to their contracts with the CSPs. Mission Owners and CSPs must refer to the memo and its Attachment A for details about fulfilling the requirement.

Cloud/data center hosting organizations are interpreted here as CSPs providing IaaS CSOs, while Application Service Providers (ASPs) are interpreted here as CSPs providing PaaS/SaaS CSOs. In both cases, the contracted CSP must obtain and provide reports from all subcontractors (e.g., data centers and CSPs hosting their CSO infrastructure) and from any CSPs whose CSOs the contracted CSP (ASP) is leveraging as an external service to provide their complete CSO.

As a condition of receiving a DOD PA, CSPs must demonstrate they can meet the requirement to produce SOC 1 Type II reports for themselves and for any subcontractors. The reporting period will be coordinated with the federal government's fiscal year.

5.4 CSP use of DOD Public Key Infrastructure (PKI)

CSPs are required to integrate with and use the DOD PKI for DOD entity authentication (e.g., a web portal that DOD and the federal government Mission Owner's privileged users log in to for configuring the CSO.)

The following sections describe how the CSP fulfills its responsibilities, with additional detail in the supporting subsections:

Impact Level 2: When a CSP is responsible for authenticating entities and/or identifying a hosted DOD information system, the CSP will use DOD PKI certificates in compliance with DODI 8520.03. CSPs will enforce the use of a physical token referred to as the "Common Access Card (CAC)" or "Alt Token" for the authentication of DOD privileged users. CSPs must use DOD Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) resources for checking revocation of DOD certificates and DOD Certificate Authorities and must follow DOD instructions and industry best practices for the management and protection of cryptographic keys.

Impact Levels 4/5: When a CSP is responsible for authenticating entities and/or identifying a hosted DOD information system, the CSP will use DOD PKI certificates in compliance with DODI 8520.03. CSPs will enforce the use of a physical token referred to as the "Common Access Card (CAC)" or "Alt Token" for the authentication of DOD privileged and DOD nonprivileged users. CSPs must use DOD OCSP or CRL resources for checking revocation of DOD certificates and DOD Certificate Authorities and must follow DOD instructions and industry best practices for the management and protection of cryptographic keys. DOD-issued PKI server certificates will be used to identify the CSP's DOD customer ordering/service management portals and SaaS applications and services contracted by and dedicated to DOD use.

Impact Level 6: When an on-premises CSO is responsible for authenticating DOD entities and/or identifying a hosted DOD information system, the CSP will use NSS PKI. CSPs will enforce the use of a physical token referred to as the CNSS NSS Hardware Token for the authentication of DOD Mission Owner and CSP privileged and nonprivileged end users. When implementing NSS PKI, CSPs must use NSS OCSP or CRL resources for checking revocation of NSS certificates and NSS Certificate Authorities and must follow CNSS/NSA instructions for the management and protection of cryptographic keys. CNSS-issued PKI server certificates will be used to identify the CSP's DOD customer ordering/service management portals and SaaS applications and services contracted by and dedicated to DOD use.

A CSP must PK enable their customer ordering/service management portals for all service offerings and their SaaS service offerings for general DOD user access at Level 4 and up or provide a customer-configurable service offering to permit PK enabling and integration with the required PKI. For complete compliance, the CSP will integrate with the DOD PKI and the federal PKI for Levels 2 through 5. For Level 6, the CSP will integrate with the NSS (SIPRNet) PKI. Both the DOD and NSS PKI are operated by DISA, and the Federal PKI is operated by GSA. PK-enabled customer ordering/service management portals may require a separate URL or dedicated application/application interface as best determined by the CSP to meet the federal government requirement.

Corresponding Security Controls: IA-2, IA-2(1), IA-2(2), IA-2(8), IA-2(12), IA-5(2), IA-7, IA-8.

NSS PKI and SIPRNet token requirements for off-premises Impact Level 6 CSPs and CSOs must be coordinated with OUSD(I) and DCSA.

5.4.1 CSP Privileged User Credentials

This section defines the identification multi-factor authentication and access control credentials the CSP privileged users must use when administering the CSP's infrastructure supporting Mission Owners' systems.

Impact Levels 2/4: The CSP must minimally implement multi-factor authentication for CSP privileged user access to administer and maintain CSP infrastructure supporting federal and DOD contracted services. The best practice of using a hardware token technology combined with a solution that uses multifactor, a one-time password or a PKI certificate, such as DODI 8520.03 Credential Strength D is preferred. However, these identity credentials minimally use a multitoken solution or a multifactor, one-time password solution such as DODI 8520.03 Credential Strength C.

Impact Level 5: The CSP must implement a strong, multi-factor authentication capability for CSP privileged user access to administer and maintain dedicated CSP infrastructure supporting federal and DOD contracted services. The strong multifactor authentication capability must be dedicated to the dedicated CSP infrastructure. These identity credentials minimally use a hardware token technology implementing a multifactor one-time password or PKI certificate solution such as DODI 8520.03 Credential Strength D. For privileged access to DOD systems, DODI 8520.03 requires that all administrators of DOD or partner-managed systems use identity Credential Strength E (i.e., hardware token PKI technology issued by an identity credential service provider that is a federal agency, an approved shared service provider under the Federal PKI Policy Authority Program, or an identity credential service provider that has been specifically approved by the DOD CIO as a Credential Strength E service provider such as DOD CAC or ALT). However, DOD is not currently enforcing this requirement on CSP infrastructure administrators/privileged users managing CSP assets.

Impact Level 6*:* The CSP must implement SIPRNet token/PKI authentication for CSP privileged user access to administer and maintain dedicated CSP infrastructure supporting federal and DOD contracted Level 6 services connected to SIPRNet.

5.5 Policy, Guidance, Operational Constraints

CSPs must follow DOD-specific policy, guidance and operational constraints as appropriate by CSPs. DISA will evaluate CSP-submitted equivalencies to any specific security control, SRG, or STIG requirement on a case-by-case basis.

5.5.1 Facilities Requirements

Impact Level 2: CSP data processing facilities supporting Impact Level 2 information will meet the physical security requirements defined in the FedRAMP Moderate baseline.

Impact Level 4: CSP data processing facilities supporting Impact Level 4 CSOs/information will meet the physical security requirements defined in the FedRAMP Moderate baseline as well as any FedRAMP+ security controls related to physical security.

Impact Level 5: CSP data processing facilities supporting Impact Level 5 CSOs/information will meet the physical security requirements defined in the FedRAMP High baseline as well as any FedRAMP+ security controls related to physical security.

Impact Level 6: DOD data on-premises processing facilities that support cloud services infrastructure and classified service offerings will be housed in facilities (designated as a secure

room) designed, built, and approved for open storage commensurate with the highest classification level of the information stored, processed, or transmitted as defined in DODM 5200.01 Volume 3, DOD Information Security Program: Protection of Classified Information.

5.5.2 CSP Personnel Requirements

The concept of cloud operations, given the shared responsibilities among multiple organizations and the advanced technology being applied within this space, can impact personnel security requirements. The ability for a CSP's personnel to alter the security controls/environment of a provisioned offering and the security of the system/application/data processing within the offering may vary based on the processes/controls used by the CSP. The components of the underlying infrastructure (e.g., hypervisor, storage subsystems, network devices) and the type of service (e.g., IaaS, PaaS, SaaS) provided by the CSP will further define the access and resulting risk that the CSP's employees can pose to the DOD mission or data. While CSP personnel are typically not approved for access to customer data/information for need-to-know reasons (except for information approved for public release), they can gain access to the information through their duties.

Access to DOD information above Impact Level 2 is limited by national affiliation. For other than U.S. Citizens or Non-Citizen U.S. Nationals as defined in 8 U.S. Code § 1408, national affiliation is defined in 22 CFR 120.15 – U.S. Person and 120.16 – Foreign Person.

The limitations by information Impact Level are as follows:

- **Impact Level 2:** CSP personnel having access to the systems processing/storing DOD public information may be U.S. Citizens, U.S. Nationals, U.S. Persons, or Foreign Persons. There is no restriction.
- **Impact Level 4/5:** CSP personnel having access to the systems processing/storing DOD CUI information or to the information itself at Impact Level 4/5 must be U.S. Citizens, U.S. Nationals, or U.S. Persons. No Foreign persons may have such access.
- **Impact Level 6:** CSP personnel having access to systems processing/storing classified information or to the information itself must be U.S. Citizens.

Corresponding Security Controls: PS-2, PS-3.

5.5.2.1 CSP Personnel Requirements – PS-2: Position Categorization

The FedRAMP Moderate baseline includes the personnel security controls PS-2, PS-3, and enhancement PS-3(3). Under PS-2, the CSP is required to "assign a risk designation to all organizational positions" and "Establish screening criteria for individuals filling those positions." Supplemental guidance states "Position risk designations reflect Office of Personnel Management (OPM) policy and guidance." The OPM position designation process considers the duties, level of supervision, and scope over which misconduct might have an effect (i.e., worldwide/government-wide, multiagency, or agency). For IT system and information access, it also considers the sensitivity level of the information accessed (i.e., non-CUI, CUI, and classified).

The OPM Position Designation Tool gives federal agencies a methodical and consistent means to determine position sensitivity for National Security Positions (e.g., positions concerned with the

protection of the nation from foreign aggression or espionage or positions that require regular access to classified information) and Public Trust Positions (e.g., positions at the High or Moderate risk levels, which include responsibility for protection of information security systems). Position risk levels are determined using the Position Designation Tool. A position may have both national security and public trust considerations that will jointly impact the sensitivity level and ultimately the type of security investigation required. The Position Sensitivity Tool will be used to determine position sensitivity, position risk levels, and investigation requirements for key CSP personnel.

DOD's primary concern is CSP personnel who have direct access to or the ability to gain access to DOD information or who have responsibilities that can affect the security of the information technology processing, storing, or transmitting that information. Under OPM policy, a person with access to CUI or classified information is designated as filling a position designated as "critical-sensitive" or "high risk". However, if the person's "work is carried out under technical review of a higher authority" (i.e., a person holding a "critical-sensitive" or "high-risk" position), the position may be designated as "noncritical-sensitive" or "moderate risk". Positions only having access to non-CUI and publicly released information could have a designation of "non-sensitive" or "low risk". All positions are considered to have some level of "public trust."

To receive a DOD PA, the CSP must demonstrate that their personnel position categorization and compliance with PS-2 are equivalent to the OPM position designations for the CSP positions similar to the "critical-sensitive" or "high risk," "noncritical-sensitive" or "moderate risk," and/or "non-sensitive" or "low risk" (i.e., access to only non-CUI and public information) position designations. These designations drive the level of screening to be established in accordance with the second half of PS-2 and for PS-3.

5.5.2.2 CSP Personnel Requirements – PS-3: Background Investigations

Under PS-3 and PS-3(3), the CSP is required to "Screen individuals prior to authorizing access to the information system" and rescreen in accordance with an organization-defined frequency. PS-3(3) addresses "additional personnel screening criteria" for information "requiring special protection," such as CUI.

The FedRAMP supplemental guidance for PS-3 required the cloud customer stipulate the type of background investigation required for CSP personnel who have access to or can gain access to information. The position sensitivity or risk level and resulting investigation may be elevated beyond the minimum requirement as determined by the Mission Owner/AO based on additional risk considerations. For DOD, the minimum designations are defined by level as described below.

Impact Level 2: CSP personnel supporting Impact Level 2 for a CSO will meet the personnel security requirements and undergo background checks as defined in OPM policy. The minimum background investigation required for CSP personnel having access to Level 2 information based on a "non-critical sensitive national security" position designation is Tier 2 National Agency Check with Law and Credit (NACLC) and Access National Agency Check with Written Inquires + Credit Check (ANACI).

Impact Level 4: CSP personnel supporting Impact Level 4 for a CSO will meet the personnel security requirements and undergo background checks as defined in OPM policy in accordance with the FedRAMP Moderate baseline, the FedRAMP+ CEs related to personnel security, and DOD

personnel security policies. The minimum background investigation required for CSP personnel having access to Impact Level 4 is Tier 3 NACLC and ANACI.

Impact Level 5: CSP personnel supporting Impact Level 5 for a CSO will meet the personnel security requirements and undergo background checks as defined in OPM policy in accordance with the FedRAMP High baseline, the FedRAMP+ CEs related to personnel security, and DOD personnel security policies. The minimum background investigation required for CSP personnel having access to Impact Level 5 is Tier 3 NACLC and ANACI with no access to customer workload/data or Tier 5 (SSBI): Critical Sensitive and Special Sensitive National Security. If Just-in-Time (JIT) administrative access is in use, the supervising administrator must have a Tier 5 clearance and the subordinate administrator can have a Tier 3 clearance.

To receive a DOD PA for Level 2, 4, or 5, the CSP must comply with the investigation requirements as listed for personnel requiring access to DOD systems and/or data. Personnel who have access to the CSP infrastructure only (i.e., at the hypervisor or below for IaaS or PaaS/SaaS CSO applications and below without access to DOD customer systems or data) must comply with OPM investigation requirements, or the CSP must demonstrate that their personnel background investigations and compliance with PS-3 and PS-3(3) are consistent with OPM investigation requirements for each position designation.

DOD suggests that the CSP request equivalent investigations to those noted above from an investigation contractor listed on the GSA Federal Acquisition Service Contractor Listing for Category 595 27 HR Support: Pre-Employment Background Investigations website. By using such a contractor and requesting equivalent investigations, the CSP can demonstrate equivalency toward receiving a DOD PA and preparing for the needed investigations following contract award.

Impact Level 6: Personnel with access to a secure room or the infrastructure supporting classified processing, or handling classified information, must meet the public trust position suitability/investigation requirements and have a security clearance at the appropriate level. Minimum security clearance is Tier 5 (SSBI) Critical Sensitive and Special Sensitive National Security. While system administrators are not usually approved for handling classified information, these privileged users are treated as having access to classified information because of their administrator duties. Therefore, these individuals require a clearance at the appropriate level for the classified information stored, processed, or transmitted.

Clearances for commercial CSP personnel are granted through the Industrial Personnel Security Clearance Process. Contracts for both on-premises and off-premises Impact Level 6 CSOs will include language related to the contractor requiring access to classified information in accordance with 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry and Federal Acquisition Regulations (FAR) Section 52.204-2 - Security Requirements. Such contractors are required to comply with NISP policies as discussed above regarding organizational facilities clearances and cleared personnel.

To receive a DOD PA for Impact Level 6, the CSP must either have a facility clearance and cleared personnel who will manage the CSO (including top-level corporate management) or demonstrate the ability to meet the requirements for these as defined in the Industrial Personnel Security Clearance Process.

For on-premises Impact Level 6, CSO facilities and personnel clearances will be handled as with any other DOD contract where the contractor needs access to classified information or as required for other purposes.

For off-premises Impact Level 6, CSO facilities and personnel clearances will be handled through the contracting process as with any other Defense Industrial Base (DIB) contractor. This process is the purview of OUSD(I) and DCSA.

Nonsystem maintenance personnel: CSP personnel who do not have electronic access to the information systems. This may include janitors or personnel who perform maintenance duties in CSP facilities but have access to the server rooms for official duty purposes. They must have a minimum-security clearance of Tier 3 Non-Critical Sensitive National Security for unrestricted access to Impact Level 4/5 information system infrastructure areas or a proper escort. Impact Level 6 security clearance as in the above section or proper escort to perform their assigned duties is required.

Corresponding Security Controls: MA-5, MA-5(5).

5.5.2.3 Mission Owner Responsibilities Regarding CSP Personnel Requirements

In addition to the above requirements, the FedRAMP Control Specific Contract Clauses v3 also states the following: "Agencies leveraging FedRAMP Provisional Authorizations will be responsible for conducting their own Background Investigations and or accepting reciprocity from other agencies that have implemented Cloud Service Provider systems."

It also states agencies are responsible for the screening process and may want to stipulate additional screening requirements. As part of the FedRAMP+ assessment, the processes used by the CSP will be evaluated and discussed in the PA as appropriate. Additionally, Mission Owners may require that some CSP personnel have clearances in the event classified information sharing may be needed at some point. This may be based on the criticality of the CSO's use case and the criticality or type of information. DOD components and/or Mission Owners must review the investigation type required for all position designations and address investigation requirements and any clearance requirements, as well as funding, in their contracts with the CSP.

5.5.2.4 Training Requirements

DOD 8570.01-M, Information Assurance Workforce Improvement Program, Change 3, January 24, 2012, describes the DOD IA Workforce Improvement Program. This manual requires DOD IA personnel to be categorized and sets experience, training, and certification standards. DOD CSPs and Mission Owners must comply with DOD 8570.01-M.

DOD Directive 8140.01 reissued and renumbered DOD Directive (DODD) 8570.01 to update and expand established policies and assigned responsibilities for managing the DOD cyber workforce. The qualification and certification standards of DOD 8570.01-M are still in effect until replaced by the DOD 8140.01 Manual. Refer to DOD Cyber Workforce (defense.gov).

CSPs operating at impact Level 6 are also required to meet the requirements of DOD 8570.01-M for their personnel. However, non-DOD CSPs at Impact Levels 2–5 are not subject to these requirements.

CSPs at all Impact Levels are required to train security personnel as described in security control AT-3. The determination to not levy DOD 8570.01-M on commercial CSPs is based on the complexities of attempting to change how a commercial CSP that serves customers outside of DOD hires and trains personnel. Commercial CSP security personnel training will be assessed for compliance with security control AT-3 as part of the FedRAMP and DOD PA assessments.

5.6 Data Spill

Per CNSSI 4009, CNSS Glossary, a data spill or "spillage" is a security incident that results in the transfer of classified information or CUI onto an information system not authorized to store or process that information.

A data spill is a cyber incident that requires immediate reporting and response from both the Mission Owner and CSP to minimize the scope of the spill and the risk to DOD data. Mission Owners will report the incident via their normal channels; the CSP must report the spill to the mission/information owner and follow the requirements in the Cyber Incident Reporting and Response section of this document. The Mission Owner will most likely detect a spillage within their own dataset, but the CSP might also detect a spillage. CSP detection may depend on a particular service offering where the CSP might have intentional access to the content of a Mission Owner's information system.

Cloud environments present a unique challenge for data spill response. Data spills in traditional IT are typically remediated or "cleaned" by sanitizing affected hardware to ensure that reconstruction of spilled data is impossible or impractical. This process requires access to physical storage media and frequently involves storage resources being taken offline until the cleanup is complete. Such loss of availability is not acceptable in a cloud environment with multiple tenants sharing the same infrastructure. CSP use of storage virtualization can generate numerous, dynamic instantiations of data and makes physical data locations difficult or impossible to ascertain. This makes physical sanitization methods nonviable for data spill remediation in cloud services. These challenges require a method for mitigating data spill cyber incidents that occur in the cloud.

Where the Mission Owner has control over the cloud environment and/or how their data is stored, as in IaaS and some PaaS CSOs, cryptographic erase is required. Additionally, DOD control of encryption keys permits Mission Owners to address data spill incidents without alerting the CSP to the presence of unauthorized data. Upon discovery of a data spill, Mission Owners should cryptographically erase unauthorized data by deleting the associated decryption key(s). Mission owners must also take any necessary steps to remove unauthorized data that may exist in an unencrypted state, such as in memory of a running virtual machine.

Due to data backup and disaster recovery methods used by Mission Owners and CSPs, data spills could affect associated storage. Data spill remediation must extend to storage media where the spilled data might migrate. All backups and mirrored storage affected by the spill must be remediated. Mission owners are responsible for ensuring that all copies of spilled data are

cryptographically erased. Timely detection, reporting, and response are key to limiting the migration of spilled data under these circumstances.

Data spills that involve unauthorized data being stored in an unencrypted state in a CSO must be mitigated by the Mission Owner using any available option to make such data unrecoverable. The response to such an event will likely be limited to methods that provide less assurance than cryptographic erase. Mission Owners that do not or cannot use encryption at rest must create data spill response procedures that enumerate all data erasure options in each CSO. Upon discovery of such an incident, a risk analysis should be performed to determine the best course of action to mitigate the risk of reconstruction of unauthorized data. This may or may not include alerting the CSP to the presence of unauthorized data to gain cooperation in mitigating the incident.

Where the Mission Owner does not have control over the cloud environment and/or how their data is stored, as in most SaaS and some PaaS CSOs, the CSP must provide capabilities within the CSO that can be activated when a spillage is detected. These capabilities should be under the control of the Mission Owner. Granular DAR encryption and data deletion capabilities at the file or database record/field level, along with cryptographic erase, should be part of those capabilities.

CSPs must provide a spillage remediation plan based on their various and specific data storage systems and processes addressing the above and Mission Owner control of capabilities for all CSOs as part of their provisional authorization package. This plan must detail how a spillage in any of the CSP's data storage facilities of offerings is able to be remediated.

Alternate innovative methods for cloud data spill protection/remediation will be assessed for equivalency to standard methods and approved if found sufficient.

Corresponding Security Controls: IR-9, MP-6.

5.7 Terminating a CSO – Data Retrieval and Destruction

When a Mission Owner terminates use of a CSO, the set of activities involved is referred to as offboarding. An offboarding process is required when a Mission Owner migrates to a new cloud service, a mission reaches end of life, a contract ends, or a CSP ceases operations. The offboarding process is split into two stages: data retrieval/migration and data sanitization or destruction.

Mission owners must prepare for an eventual CSO offboarding, and CSPs must support the capability in a timely manner.

Upon request by the Mission Owner, the CSP will make all Mission Owner data stored in a CSO available for electronic transfer out of the CSP environment in a standard, nonproprietary format. CSPs must also make available all audit logs relevant to the Mission Owner's use of the CSO. This includes all audit content specified by the AU-2 security control for the period specified by AU-11. CSOs that enable Mission Owners to download their data on demand and delete or request destruction of data may not require specific CSP action to fulfill this requirement. Each Mission Owner may also request different means of data transfer (for example, as called out in the SLA), at its discretion.

Cryptographic erase provides a high-assurance way of ensuring data at rest can no longer be read. Upon successful transfer of data out of a CSO, Mission Owners with data that is encrypted at rest must cryptographically erase all such mission data and take action to ensure that no data remains in the CSO in an unencrypted state.

All backups maintained in the CSO's infrastructure from which the Mission Owner is departing must also be cryptographically erased. Mission Owners should also request that all mission data be deleted or made logically inaccessible as per normal CSP procedure for departing customers. Upon verification of successful Mission Owner transfer of data, CSPs must immediately delete or otherwise make all Mission Owner data irretrievable. CSPs remain responsible for sanitizing or destroying all storage devices that held DOD data at the hardware's end of life even after offboarding is complete.

DOD Mission Owners using non-DOD service offerings must be capable of migrating their data at any time. This means that Mission Owners must have the ability to receive their data from a cloud service on short notice. This capability can be supported in the form of available local storage infrastructure or a cloud service offered by a different CSP capable of accepting data in a short time frame. This is to ensure that Mission Owners can quickly retrieve their data in case of a sudden shutdown of a CSO. (e.g., a CSP declares bankruptcy and plans to shut down services). This concern is also mitigated by the Mission Owner's use of effective backup procedures.

Corresponding Security Controls: MP-6.

5.8 Reuse and Disposal of Storage Media and Hardware

CSPs will ensure that no residual DOD data exists on all storage devices decommissioned and disposed of, reused in an environment not governed by an agreement between the CSP and DOD, or transferred to a third party as required by the FedRAMP selected security control MP-6.

Impact Levels 4/5: CSPs may not reuse or dispose of storage hardware until all DOD data has been successfully removed. The CSP will minimally ensure this by "purging" all data on devices prior to decommissioning, disposal, reuse, or transfer in accordance with NIST SP 800-88, Revision 1, Guidelines for Media Sanitization. Devices that are unable to be cleared or purged must be physically destroyed, as defined in NIST SP 800-88 Rev 1. When there is any doubt to the success of the cleared or purged process, the storage device must be destroyed in accordance with NIST SP 800-88 Rev 1.

Impact Level 6: On-premises CSPs may not dispose of or reuse storage hardware at a lower sensitivity or classification level but will ensure classified data is irretrievable from decommissioned devices by sanitizing them in accordance with NSA/CSS Storage Device Declassification Manual 9-12.

Corresponding Security Controls: MP-6.

5.9 Architecture

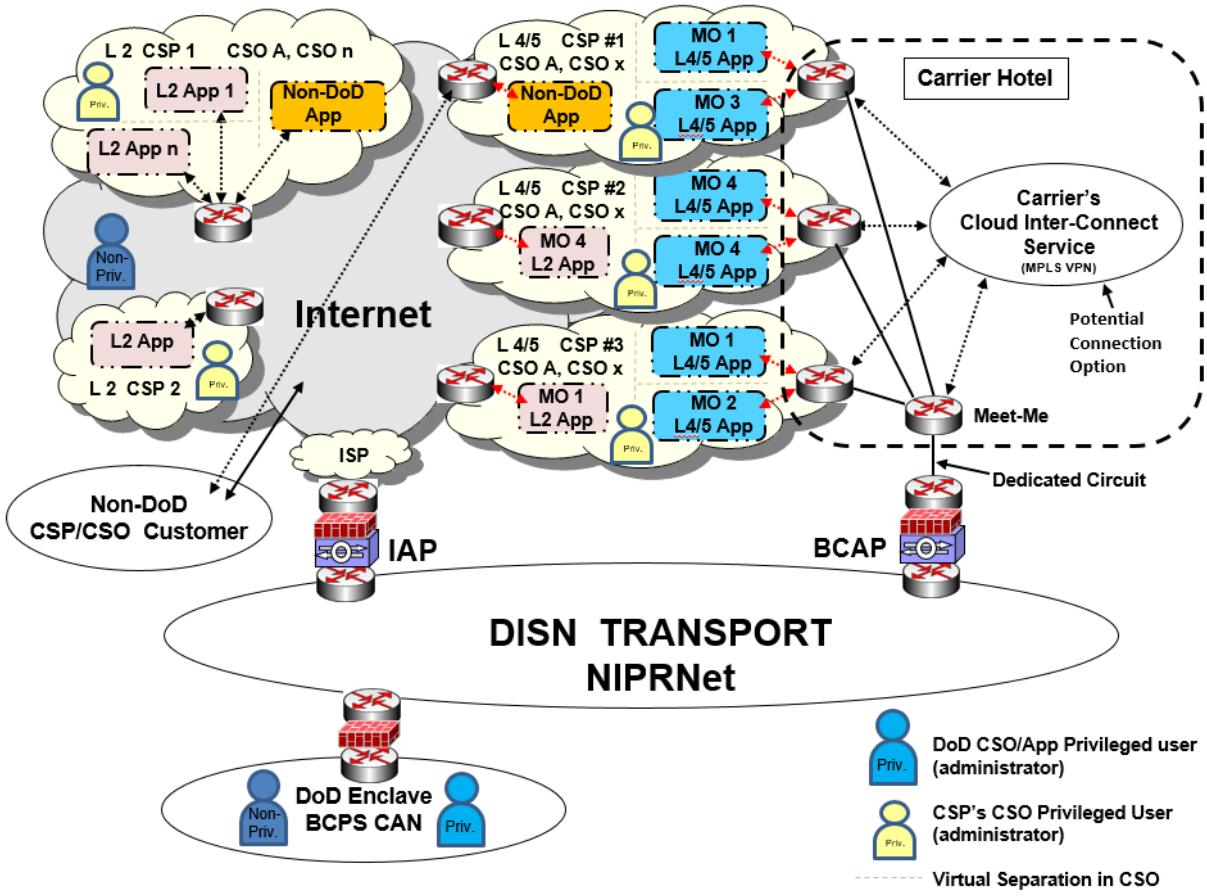
This section of the Cloud Service Provider SRG provides guidance on the various architectural considerations related to DOD's use of DOD and commercial cloud services in the following areas:

- The connection between the CSP's infrastructure/network and the DISN.
- CSP service protections and integration into required DODIN Cyberspace Defense and access control services.
- Mission system/application protections and integration into required DODIN Cyberspace Defense and access control services.

DOD's use of commercial cloud services means the DOD joins an ecosystem of internet-connected CSPs/CSOs. While DOD leverages internet-connected CSOs for the dissemination or processing of public information (Impact Level 2), DOD also leverages private connectivity to the same CSOs for the protection of sensitive DOD information (i.e., CUI at Levels 4 and 5). Additionally, DOD Mission Partners that are not native to NIPRNet will need to leverage internet-connected CSOs for their Impact Level 4/5 processing (possibly under waiver) or will need to implement their own private connectivity.

Figure 5-8: shows the overall architecture of the cloud ecosystem into which NIPRNet is connected that consists of off-premises, non-DOD-private commercial, and federal CSPs/CSOs. Any of the CSP/CSO clouds in the diagram may be a commercial CSO or a CSO operated/offered by a non-DOD federal agency. This diagram reenforces that every non-DOD-private commercial and/or federal CSP/CSO is accessible from the internet even if the CSO has a Level 4/5 PA and is connected to NIPRNet via private connections. It also demonstrates that these CSPs/CSOs support non-DOD customers. This figure focuses on NIPRNet connectivity to commercial/federal CSOs for most mission use cases. It does not show all possible situations or use cases. Additional figures may be provided in future releases of the Cloud Service Provider SRG.

Figure 5-8: NIPRNet/Commercial/Federal Cloud Ecosystem



5.9.1 Cloud Access Point (CAP)

In general, a CAP is required to mitigate risks to the DISN (or other DOD network) posed by connecting commercial CSOs to it except under certain restrictions. A CAP is a system of network boundary protection and monitoring devices (e.g., firewall, IPS, IDS, proxy, etc.), otherwise known as a cybersecurity or IA stack, through which CSP infrastructure and networks will connect to the network the CAP protects. The DISN is a protected network that includes NIPRNet, SIPRNet, and other DISN-based Mission Partner/COI networks.

The primary purpose of a CAP is to protect the DOD network from, and detect, unauthorized network access from the CSP's infrastructure, CSO management plane, CSP's corporate networks, CSP's connections to the internet, and unauthorized traffic generated from compromised Mission Owner systems/applications and virtual networks.

The secondary purpose is to protect the DODIN (i.e., DOD information) in general by facilitating protected connections for network users to access Impact Level 4–6 Mission Owner systems/applications instantiated on IaaS/PaaS, or using SaaS, and the information stored and processed there, without exposing that traffic to the internet. These purposes also apply to any CAP on any other DOD, Mission Partner, or COI network to protect those networks and the sensitive information they contain.

A CAP does not protect the cloud-based application or the network enclave (physical or virtual) in which it resides. Each Mission Owner having control over what is built in the application's virtual environment in I/PaaS must provide for the protection of their application and virtual network enclave. In the case of CSOs such as P/SaaS where the Mission Owner does not have control over what is built in the P/IaaS application's environment, the CSP is responsible for the protection of the application and the network enclave (physical or virtual) in which the application resides.
CAP architecture will change depending on whether the CSO infrastructure is on-premises or off-premises and the services transiting it. The concepts of Internal CAPs (ICAPs) for on-premises CSOs and Boundary CAPs (BCAPs) for off-premises CSOs are detailed below with a focus on how these are implemented to protect the DISN. Some CAPs will leverage existing infrastructure, and some will be a new capability. CAP architecture may also change depending on the DODIN or COI network it is protecting.

The basic capabilities that any CAP must provide in support of DODIN cyber defense are as follows:

- A firewall capability that will only permit inbound (to DISN) responses to outbound (from DISN) requests to the CSO (all permitted) while denying all traffic originating in the CSO or its management plane, except for specifically authorized traffic from the CSO to specific DOD endpoints on the DISN (permit by exception, deny by default). This will address the potential for unauthorized DODIN/DISN access from the CSO management plane or from a compromised CSO.
- An intrusion detection capability to detect firewall failure, unauthorized traffic, and malware or other malicious traffic conveyed in unencrypted traffic.
- In the event voice and/or video over IP (VVoIP) traffic consisting of the SIP-TLS and SRTP protocols (or their unsecure versions, which are not permitted) traverse the CAP, a session border controller (SBC) capability must be implemented. The SBC capability must be implemented in a back-to-back-SIP user agent/proxy mode, so a TCP/UDP port is not statically opened to inbound signaling. The SBC capability must also dynamically manage the randomly selected ephemeral UDP ports for media (SRTP) such that these IP ports are only opened for the duration of the communications session. Additionally, the SBC capability must act as a SIP/SRTP intrusion detection system to detect and report unauthorized activities, malformed/dropped packets, etc.

The above capabilities must provide feeds to the DODIN boundary Cyber Defense capabilities so anomalies can be detected and correlated with other anomalies on the network and information systems.

The remainder of this section will define the CAP requirements for DISN-connected CSOs. These concepts can also be applied to other networks that do not use DISN transport and are not behind the DISN IAPs.

Corresponding Security Controls: SC-7, SC-7(3), SC-7(4).

5.9.1.1 Boundary CAP (BCAP) Level 4/5

A BCAP is required to connect off-premises non-DOD (commercially or governmentally) owned and operated CSOs to the DISN (or other DOD networks). A BCAP will interconnect the network it protects with multiple CSP networks that offer private connectivity services. A BCAP does not provide direct internet access to or from CSP CSOs, the mission applications built upon them, or network users.

In general, a BCAP will provide the following protections:

- Provides DISN perimeter defenses and cyber defense sensing for traffic to and from applications hosted in the CSO.
- Protects the DODIN (i.e., DOD missions and information within the DISN), along with the DISN and its network services, from incidents that affect a particular CSP's infrastructure or supported missions.
- Protects DOD systems/applications instantiated in one CSP's infrastructure from incidents that affect a different CSP's infrastructure or supported missions.

A DISN BCAP is a DISN boundary intended to protect the enclave and information system, which is the DISN and its other interconnected enclaves. The DISN is on the inside or protected side of the boundary. Likewise, Mission Owner systems/applications implemented in I/PaaS or using P/SaaS are considered enclaves that require enclave boundary and demilitarized zone (DMZ) protections (alternate solutions will be considered on a case-by-case basis). These are on the outside or unprotected side of the boundary. Therefore, Mission Owner systems/applications implemented in I/PaaS as well as P/SaaS applications must protect themselves. This must be accomplished as close to the application enclave boundary as possible. Multiple Mission Owner systems/applications implemented in IaaS and PaaS where the Mission Owner has control over the VMs and environment must include virtual enclave boundary and DMZ protections for their application, or they can be protected by a virtual datacenter security stack (VDSS) and managed through a virtual datacenter management suite (VDMS). Mission Owner use of PaaS or SaaS where the Mission Owner does not have control over the VMs and environment must rely on the enclave boundary and DMZ protections afforded by the CSP for their CSO or leverage an alternative solution (e.g., a third-party CSO such as a cloud access security broker [CASB] service having minimally a FedRAMP Moderate PA).

P/SaaS CSOs are typically connected to the internet and thus must have enclave boundary and DMZ protections within their infrastructure to protect their customer's data from internet threats. DOD trusts this is the case and validates it through the FedRAMP P-ATO and DOD PA processes.

5.9.1.1.1 NIPRNet BCAP

The primary purposes of the NIPRNet BCAP are to:

- Protect the NIPRNet from the CSPs/CSOs.
- Provide private connectivity to the CSP's networks from the NIPRNet in support of NIPRNet user connectivity to Impact Level 4/5 cloud-based applications and services.

The implementation of the DISN BCAP capability for NIPRNet is ultimately a DISA responsibility as part of its mission to protect the DODIN and DOD information. Per the 15 December 2014 DOD CIO memo, initial capability may temporarily be provided by DOD components other than DISA, as approved by the DOD CIO, while the intent is for DISA to implement DISN BCAPs as an enterprise-wide DISN service. This requirement is applicable to Boundary CAPs to the NIPRNet, not ICAPs. Specific CAP architectural requirements are beyond the scope of this SRG and will be published separately in the Secure Cloud Computing Architecture (SCCA) Functional Requirements document (FRD).

The NIPRNet BCAP must be implemented as a system of hyper-redundant, dual-homed, geographically disbursed, high-availability, high-capacity cybersecurity stacks and meet-me points so the BCAP system can manage the throughput required to handle all the applications expected to migrate to commercial cloud. It provides connectivity between DISN users and multiple off-premises Level 4/5 CSOs. It also facilitates user connections to these CSOs from the internet through the DISN IAPs for internet-facing applications (IFAs).

Impact Level 2: The NIPRNet BCAP is not used because off-premises CSP infrastructure having a Level 2 PA is directly connected to the internet. All traffic to and from a Level 2 CSO serving Level 2 missions and their mission virtual networks will connect via the internet. NIPRNet users access these CSOs and applications via the DISN IAPs, while internet-based users access them directly. Mission Owner applications implemented in I/PaaS CSOs where the Mission Owner has control over the environment must provide their own enclave boundary and DMZ application protections or leverage an enterprise-level application protection service (i.e., the VDSS/VDMS portion of the SCCA) instantiated within the same CSO. VDSS/VDMS may be provided by DISA, a DOD component, or the Mission Owner. SaaS CSOs must provide their own enclave boundary and DMZ application protections to which a Mission Owner may add protection services (e.g., CASB). Alternately, Level 2 IFAs may be implemented in a Level 4/5 CSO and thus will connect to the internet directly or through the IAPs and NIPRNet BCAP. Refer to Impact Levels 4/5 below. All IFAs providing access to publicly released information, along with some IFAs providing access to low confidentiality private information, should migrate to a Level 2 CSO rather than a Level 4 or 5 CSO. This will not only reduce the load and required capacity on the BCAP infrastructure and IAPs but will also reduce the attack surface of the NIPRNet and permit the DOD and Components to realize the greatest cost savings and support other mandated cost-saving initiatives.

Impact Levels 4/5: Except as approved (waivered) by DOD CIO, all DOD traffic from NIPRNet (or other DISN-based COI network) to and from off-premises CSP infrastructure serving Level 4 and Level 5 missions and the mission virtual networks must traverse one or more NIPRNet BCAPs. No direct Impact Level 4/5 traffic is permitted to/from the internet except via the NIPRNet IAPs and DMZ capabilities provided by the Mission Owner, a DOD component, or DISA. The BCAP or an attached meet-me point provides for direct physical or logical connectivity between the DISN and CSP's network through which the CSO is accessed. Physical connectivity is established using a direct fiber optic connection between the DISN meet-me point router and a nearby CSP network router. Logical connectivity is established using dedicated long-haul circuits, Private IP VPN services, a FedRAMP authorized multi-CSP/customer interconnection service, or a point-to-point IPsec VPN. These connections can also support the transport of IPsec VPN connections originating within the CSP's network infrastructure and/or Mission Owner's virtual networks. This includes the production plane for nonprivileged user access and the management plane for privileged user access and deployed IA/cybersecurity defense tool connectivity to internal DISN

native cybersecurity defense monitoring systems. High-availability Mission Owner systems and their supporting CSP network infrastructure must connect through two or more NIPRNet BCAPs.

The NIPRNet BCAP will also provide the following functions:

- Serves as an authorized DOD DMZ for IFAs and mission systems in Level 4/5 CSOs, providing the DISN-facing DOD IP addresses used by the mission system/application are authorized DOD DMZ IP addresses. Mission Owner applications in I/PaaS must provide their own DMZ application protections or leverage an enterprise-level application protection service (i.e., the VDSS/VDMS portion of the SCCA) provided by DISA or a DOD component in the cloud. A BCAP does not support/provide direct internet access to a Level 4/5 CSO. Such access must be via the NIPRNet IAPs.
- May terminate physical or logical connections from the internal side of a DOD component's DMZ such that the DOD component's existing DMZ protections may be leveraged for their IFAs.

Level 5 CSP/CSO infrastructure/applications and DOD Mission Owner applications must be designed so they do not depend on internet-based resources that would require traffic to traverse the IAPs to/from the internet to make the CSO function. The CSO and DOD Mission Owner applications connected through a BCAP must be able to function fully, serving NIPRNet-connected users in the event DOD decides to cut off NIPRNet access to the internet. In this situation, internet-connected users will not be able to use the Level 5 service/resource. Mission Owners that need this restriction for Level 4 CSOs must add the requirement to their SLA/contract.

Certain missions that handle CUI (i.e., Impact Level 4/5 applications) primarily support internet-based users rather than NIPRNet-based users. For this reason, the Mission Owners of such applications may want to seek DOD CIO approval (waiver) to host their application and information in a CSO with a DOD Impact Level 4/5 PA but connect it directly to the internet rather than forcing their internet user traffic through the IAPs and BCAP. If approved, the Mission Owner must protect their application and information in accordance with the protection defined above for Impact Level 2 applications.

5.9.1.1.2 CSP Support for BCAP Connectivity

To support BCAP connections between DOD and an off-premises Level 4/5 CSP, the CSP must offer a private connection service to the CSO that does not traverse the internet. The CSP's network must include a point of presence (PoP) in a carrier-agnostic commercial network interconnection facility or commercial carrier's collocation facility where an existing DISN PoP/BCAP meet-me-point is located. A physical connection within the facility will be installed between the two PoPs, providing a direct private connection between the DISN BCAP and the CSP's network over which the CSO will be accessed along with supporting services. If reliability is a requirement for access to the CSO, the interconnections must be implemented in at least two geographically disbursed network interconnection/collocation facilities.

As a condition for a DOD Level 4 or Level 5 PA, the CSP must offer the private connection service for access to the CSO. DOD recognizes that the CSP may not have one or more PoPs collocated with a DISN BCAP meet-me point. Therefore, a CSP network PoP will not be required for obtaining the PA. Instead, there must be a willingness to install such a PoP, negotiate a mutually

agreeable location for collocating the DISN and CSP PoPs, or use an approved intermediary cloud interconnection service (having its own DOD PA). Associated costs will be negotiated between the Mission Owner and CSP. If a new DISN meet-me PoP is required, DISA must be included in such negotiations. Notice of this potential situation must be provided during the PA assessment phase. The negotiations will occur in the planning stage for the BCAP connection based on a contract between the CSP and their first Mission Owner. Mission Owners may also stipulate that the CSP must have/install a PoP collocated with one or more DISN meet-me points.

5.9.1.1.3 CSP/CSO Network Connectivity to Internet and BCAP

Section 5.10, Architecture, and Figure 5-8: NIPRNet/Commercial/Federal Cloud Ecosystem, depict the reality that CSPs/CSOs having a Level 4/5 PA that are connected to the NIPRNet via a NIPRNet BCAP are also connected to the internet.

As a condition for a DOD Level 4 or Level 5 PA, when the CSP's network supporting a DOD-contracted CSO is privately connected to the NIPRNet via a NIPRNet BCAP (or other DOD network via their BCAP) and the internet, the CSP must provide evidence that the CSP's network or the CSO cannot provide a path from the internet to the NIPRNet (or other network), thus creating a back door to a DOD network.

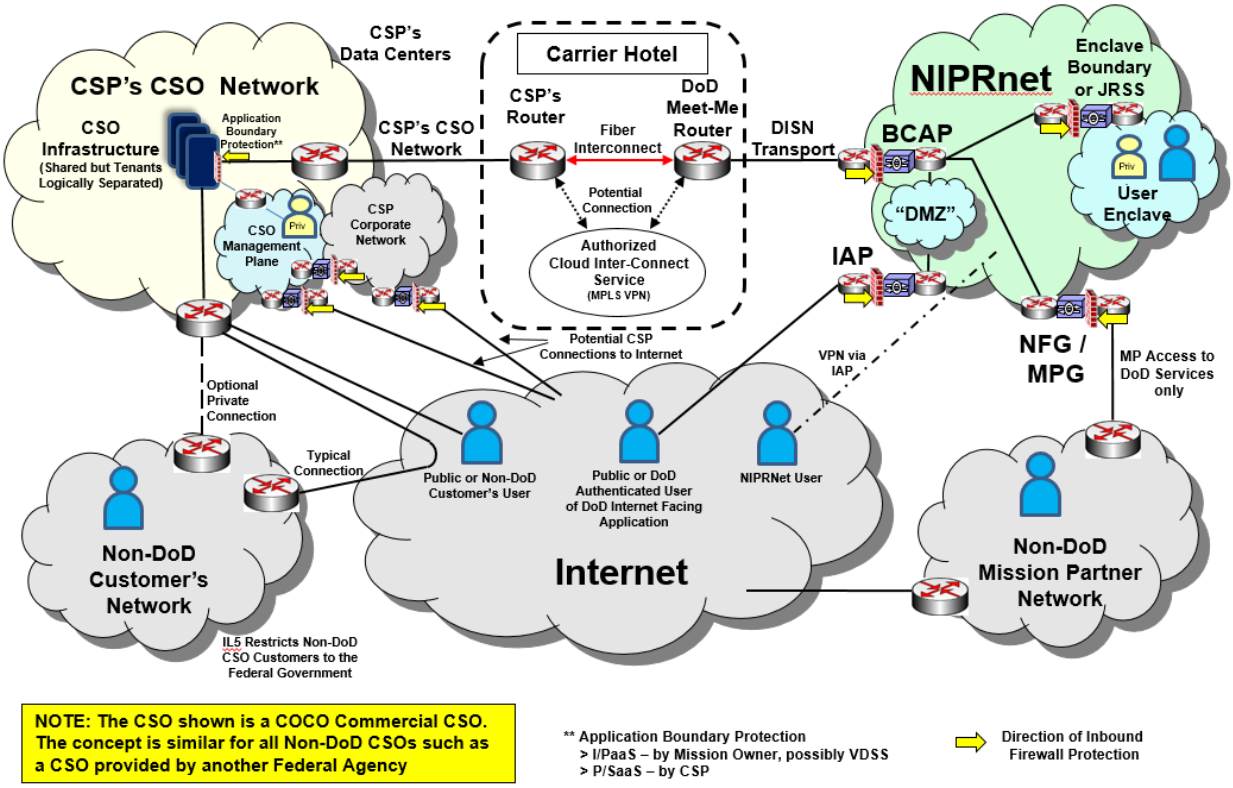
An additional or associated consideration is the robustness of the CSP's required boundary protection (defense-in-depth security/protective measures) implemented between the internet and the CSO for its protection from internet-based threats. This protection is expected to be different depending on whether the CSO is I/PaaS or P/SaaS and whether the Mission Owner has control over their portion of the CSO. Refer to Section 5.9.3, CSP Service Architecture, and Section 5.10, DOD Contractor/Component Mission Partner Use of CSOs, for details.

Figure 5-9 notionally depicts the method by which off-premises, nonprivate, non-DOD CSOs are connected to NIPRNet and other networks and how various user communities access the CSO. The following are important takeaways from the diagram:

- The CSP's network through which the CSO is accessed is connected to NIPRNet through the BCAP and meet-me points, creating a private connection. This connection is typically a fiber jumper between the meet-me router and the CSP's network router. This connection may optionally be made via an authorized Cloud Inter-Connect Service, providing access to multiple CSPs' CSOs.
- The CSP's CSO will be connected to the internet to support connections from non-DOD customers of the CSO. These customers may optionally connect via their own private connections. If public users are supported, they will connect via this internet connection.
- The CSP's CSO will be managed from the CSP's management plane, which may be connected to the CSP's corporate network, one or both of which will have one or more connections to the internet. Both may extend worldwide, touching multiple locations/CSO instances and other CSOs.
- NIPRNet users accessing DOD services from the internet, including those based in the cloud, will VPN into the NIPRNet to access these services.

- Non-DOD and public users accessing DOD IFAs from the internet will do so via the IAPs (and DOD DMZ as applicable). This includes authenticated users of DOD IFAs. Direct internet access is only permitted under DOD CIO approval (CAP Waiver).
- Non-DOD Mission Partner networks accessing DOD services, whether cloud-based or not, access the NIPRNet via the NIPRNet Federal/Mission Partner gateway(s). Access to the CSO for their own use will be the same as the non-DOD customer's network.

Figure 5-9: Notional Connectivity – Off-Premises, Nonprivate, Non-DOD CSOs (Commercial/Federal) (NIPRNet Impact Level 4/5)



5.9.1.2 Internal CAP (ICAP)

Impact Levels 2/4/5: ICAPs will be implemented for on-premises commercially owned and operated CSO connectivity to the DISN if the CSO management plane has connectivity to external networks that bypasses native NIPRNet enclave and external boundary (IAP) protections. All NIPRNet (or other unclassified COI network) production traffic to and from on-premises commercially owned and operated CSP infrastructure serving Level 2, 4, and 5 missions and the mission virtual networks must traverse an ICAP.

An ICAP is a DISN boundary consisting of a cybersecurity stack that protects the DISN (or other DOD network) or the data center network to which the CSO is connected (inside/protected side of the boundary) from, and provides detection of, unauthorized network access from the CSP's infrastructure (outside/unprotected side of the boundary), externally connected CSO management plane, CSP corporate networks, CSP connections to the internet, and compromised Mission Owner

systems/applications and virtual networks. Typically, one ICAP is required for each physical CSO infrastructure instance.

An ICAP is required to mitigate vulnerabilities and risks associated with implementing a commercial CSP's CSO infrastructure on-premises (i.e., located inside the B/C/P/S physical or virtual "fence line") when that infrastructure is managed by the CSP from their off-premises corporate CSO management centers using non-DOD controlled workstations and infrastructure that will most likely have some connectivity to the CSP's corporate network and/or the internet. The connection between the CSO management centers and the on-premises CSO's management plane is expected to traverse an IPsec tunnel across NIPRNet, its IAPs, and the internet or traverse a dedicated "side-door" connection using a dedicated circuit, a commercial carrier's private IP VPN service, or restricted internet service provider (ISP) connection. ISP connections, across which the CSP must VPN, must not provide inbound or outbound access to/from the CSO management plane to/from the open internet. This requirement also applies if the CSO management plane is locally dedicated to the CSO and managed on-premises but with an external connection to the CSP's corporate or similar network.

The ICAP will be configured to pass authorized production traffic (i.e., required protocols and services on their approved IP ports) for mission applications using the CSO while blocking all access to DISN or the data center network to which the CSO is connected from the CSO management plane.

The architecture of ICAPs may vary and will be developed based on the location of the CSO infrastructure on the BCPS, existing infrastructure, and other factors. An ICAP minimally consists of firewall and IDS/IPS functions but may leverage existing capabilities such as the cybersecurity stack protecting a DOD data center (today, e.g., DECC), JIE CDC, or Joint Regional Security Stack (JRSS). An ICAP may have special capabilities to support specific missions, CSP types (commercial or DOD), or cloud services. Because the CSP infrastructure and ICAP are both on-premises connected directly to the NIPRNet or indirectly via a DOD data center network, the full suite of BCAP boundary protections is not needed.

When using the cybersecurity stack protecting a DOD data center today (e.g., Defense Enterprise Computing Center [DECC]) or JIE CDC in the future as an ICAP, the CSO must be connected in such a manner that both the DISN and data center network are protected from the CSO management plane.

ICAP implementation and the connection of on-premises CSP infrastructure to the NIPRNet will follow normal NIPRNet connection approval guidance and requirements as with any NIPRNet enclave or application infrastructure in a DOD data center.

An ICAP is not required if the CSO is managed under either of the following conditions:

- The CSO management plane is a closed network directly part of the CSO infrastructure having no side-door or back-door connections to non-DISN networks.
- The CSO management plane is a NIPRNet enclave or part of one that only has connectivity to external networks such as the internet or CSP corporate network via, and visible to, the native NIPRNet boundary protections and IAPs. While CSP personnel may VPN to their corporate network from their workstation, a point-to-point VPN may not be established

between the CSP's network and the CSO management plane. The latter will require the establishment of an ICAP.

Additionally:

- CSP personnel manage the CSO from a location on a DOD installation/BCPS.
- The CSP personnel are issued government-furnished equipment (GFE) from which they perform their CSO management duties if these workstations can access the NIPRNet.
- CSP personnel may not use the same GFE to manage the CSO that is used to perform general business functions such as email or those that might require surfing the internet.
- The CSP personnel are issued CACs for installation/BCPS access and access to their GFE and NIPRNet.

Figure 5-10 below notionally depicts the method by which on-premises DOD private CSO infrastructure is connected to NIPRNet when the CSO is managed from a contractor's off-premises management plane. This may apply to contractor owned/operated or government owned/contractor operated CSO infrastructures. The following are important takeaways from the diagram:

- If the on-premises (private) CSO infrastructure is managed from an off-premises non-NIPRNet CSO management plane or contractor enclave, an ICAP is required. This is due to the likely connection to a corporate network, and both may have one or more connections to the internet.
- Connection from the off-premises CSO management plane to the CSO infrastructure may be via an encrypted tunnel that traverses any of the following connections: an IAP, the NIPRNet, the data center boundary (if in line with an IAP), or a dedicated ISP circuit.
- NIPRNet users accessing DOD services from the internet including those based in the cloud who will VPN into the NIPRNet to access these services.
- Non-DOD and public users accessing DOD IFAs from the internet will do so via the IAPs (and DOD DMZ as applicable). This includes authenticated users of DOD IFAs.
- Non-DOD Mission Partner networks accessing DOD services, whether cloud based or not, access the NIPRNet via the NIPRNet Federal/Mission Partner gateway(s). Access to the CSO for their own use will be the same as the non-DOD customer's network.

Figure 5-10: Notional Connectivity: On-Premises DOD Private CSOs and Off-Premises Management Requiring ICAP (NIPRNet Impact Level 4/5)

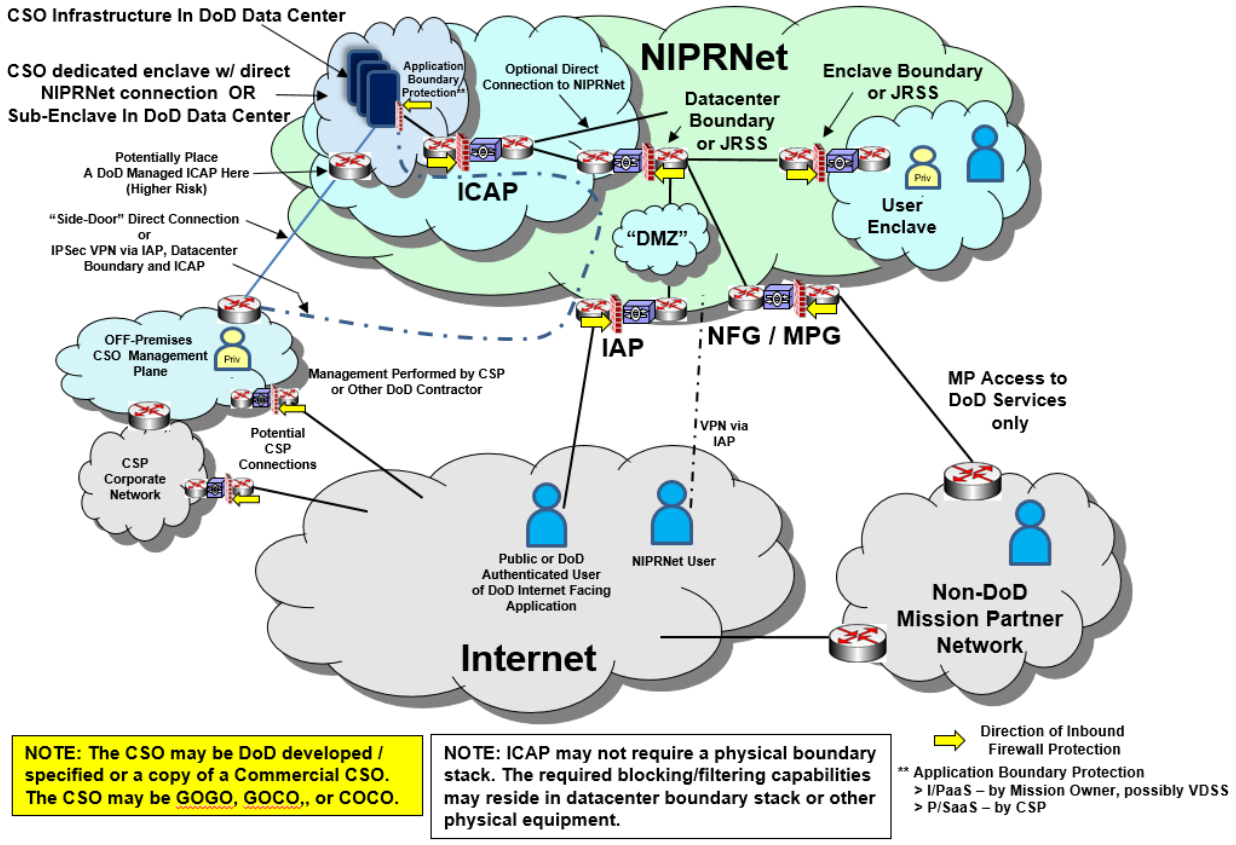
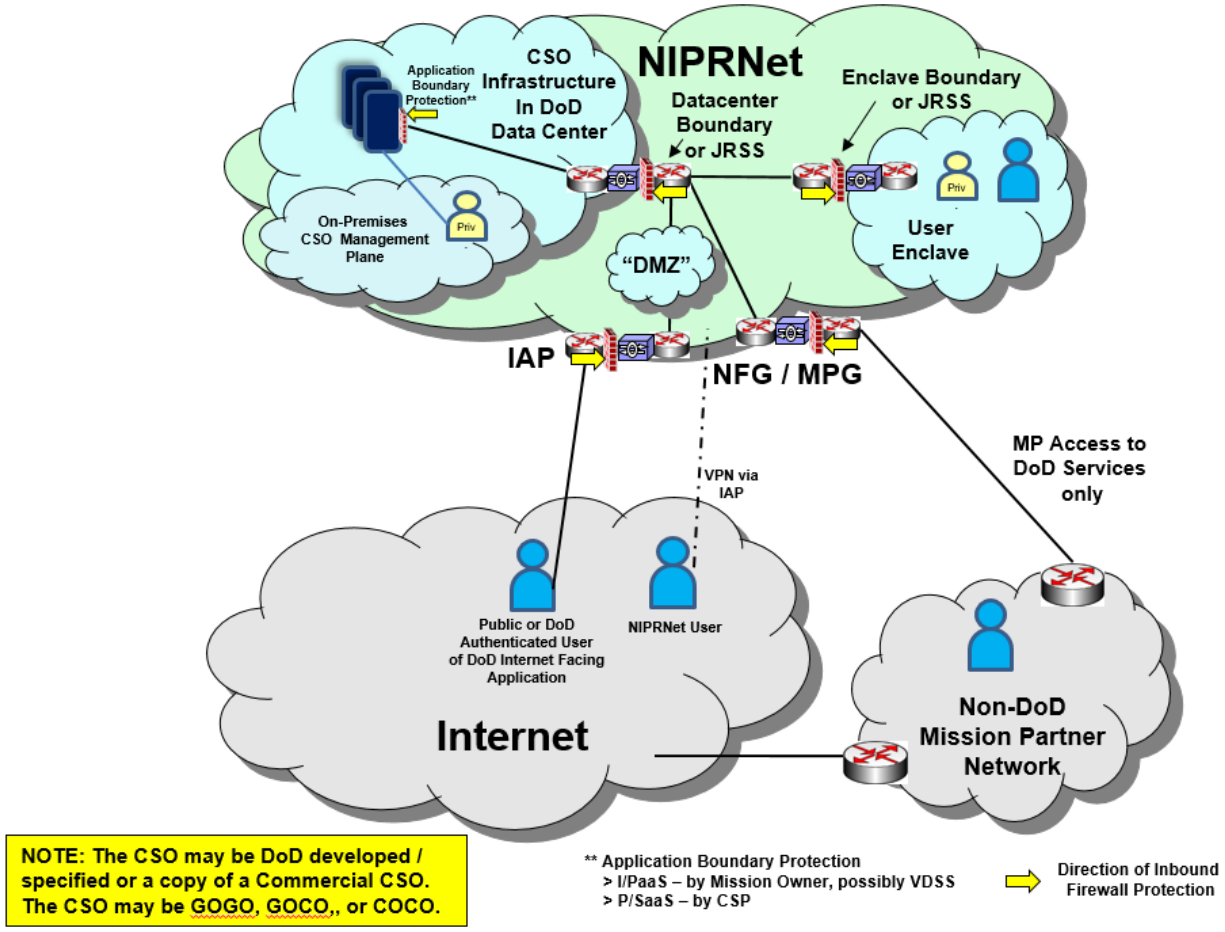


Figure 5-11 below notionally depicts the method by which on-premises DOD private CSO infrastructure is connected to NIPRNet when the CSO is managed from an on-premises management plane. This contrasts with being managed from an off-premises management plane. The following are important takeaways from the diagram:

- ICAP is not needed if CSO management is performed from an on-premises NIPRNet enclave.
- (Not depicted) If the CSO infrastructure is directly connected to the NIPRNet, a data center enclave boundary must be provided.

Figure 5-11: Notional Connectivity: On-Premises DOD Private CSOs & On-Premises Management (NIPRNet Impact Level 4/5)



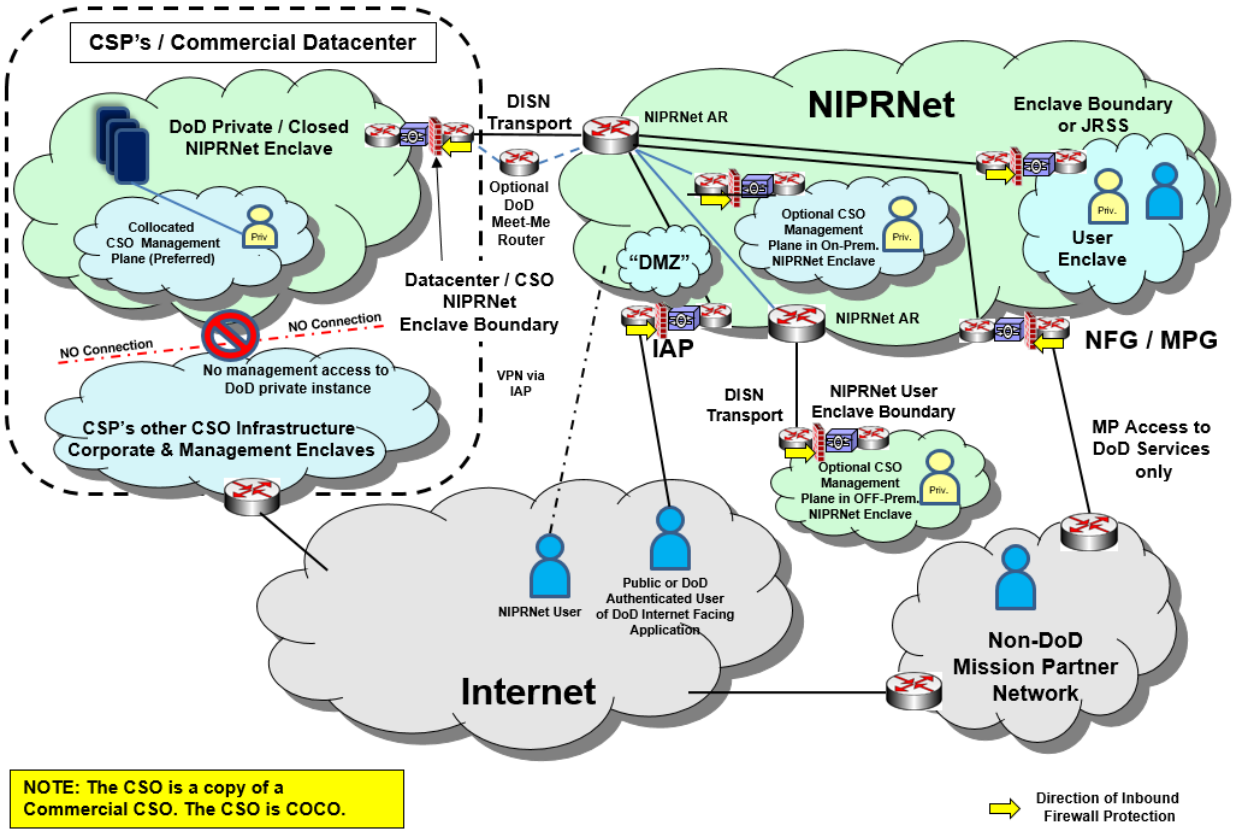
5.9.1.3 Virtually On-Premises Architecture NIPRNet Level 4/5

The "virtually on-premises" concept is discussed above in Section 5.2.1.1, DOD Off-Premises vs. On-Premises vs. Virtually On-Premises. Figure 5-12 notionally depicts the method by which a virtually on-premises architecture can be achieved. The following are important takeaways from the diagram:

- The CSO infrastructure is DOD private in a closed NIPRNet enclave that is off-premises.
- DISN transport is extended to this enclave optionally via a meet-me point. The use of a meet-me point may invoke additional traffic separation requirements depending on the specific off-premises location in relation to the meet-me location and if the hosting parties' network is used.
- The CSO network enclave is protected with DOD NIPRNet data center enclave protections or equivalent, including enclave firewall and Intrusion Prevention System (IPS).
- The DOD private CSO infrastructure is managed from the same or another properly protected NIPRNet enclave.

- No management of the private CSO infrastructure may be performed from the CSP's management plane used for any other CSO offered. No such connection is permitted in this scenario. Any connection between the private CSO infrastructure and a nondedicated management plane enclave negates the virtually on-premises construct and requires the connection to the NIPRNet to traverse a BCAP.

Figure 5-12: Notional Connectivity: Virtually On-Premises DOD Private CSOs & Management (NIPRNet Impact Level 4/5)



5.9.1.4 SIPRNet ICAP

DOD SECRET enclaves and virtual networks instantiated in DOD on-premises Impact Level 6 CSOs will be considered an enclave within the DOD provider network (i.e., the SIPRNet).

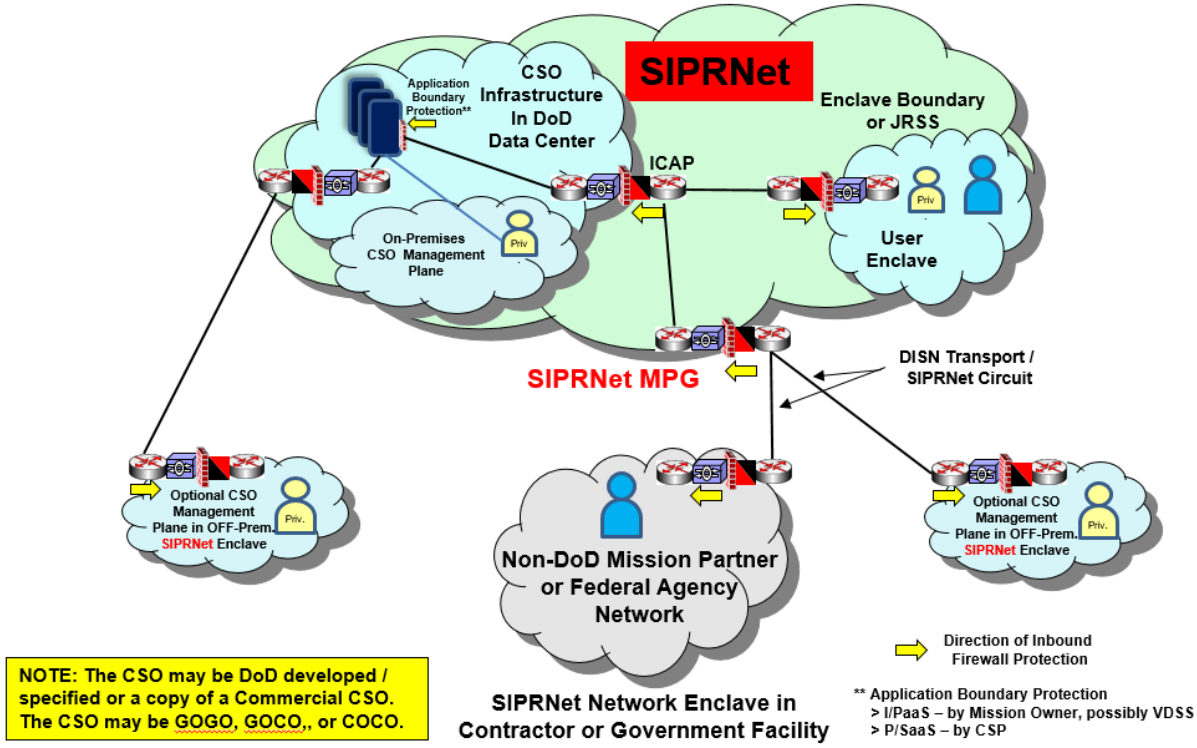
Because DOD on/off-premises Impact Level 6 CSOs and their supporting infrastructure, including management networks, are required to be one or more closed SIPRNet enclaves, they can be on-premises (physically or virtually) for the purposes of this Cloud Service Provider SRG due to the concept of extending the virtual "fence line" or SIPRNet boundary around such DOD enclaves. These enclaves must comply with all SIPRNet connection approval requirements, which include the appropriate enclave boundary protections and cyberspace defense requirements. The DOD Mission Owner systems/applications instantiated in these Impact Level 6 CSO enclaves will be assessed and authorized in the same way as any other DOD SIPRNet enclave connection.

ICAPS are required as they are for NIPRNet connections to CSOs.

Figure 5-13 below notionally depicts the method by which an on-premises Impact Level 6 CSO would be connected to SIPRNet. The following are important takeaways from the diagram:

- The management plane is also on SIPRNet within the same or another SIPRNet enclave.
- ICAP is required.
- Non-DOD Mission Partners or other federal agencies will access the CSO via the SIPRNet Mission Partner Gateway.
- If the CSO is managed from a SIPRNet enclave not collocated with the CSO infrastructure, connections to the CSO will be via the SIPRNet Mission Partner Gateway or the CSP may institute a private connection using black transport.

Figure 5-13: Notional Connectivity: On-Premises DOD Private CSOs & On/Off -Premises Management (SIPRNet Impact Level 6)



5.9.1.5 Mission Partner Environments or Communities of Interest Network Cloud Access Points

Mission Partner refers to DOD components, federal agencies, and potentially their contractors operating networks that include DOD and other entities. This section does not include or refer to warfighting coalition partners or the networks they use or that are implemented for them.

Mission Partner Environments (MPEs) include Mission Partners that use networks other than NIPRNet or SIPRNet (e.g., DREN) and Mission Partner COIs that use network overlays and extensions that leverage (e.g., ride on or overlay) the NIPRNet or SIPRNet (e.g., MilCOI). Additionally, DOD component Mission Partners (e.g., commissaries; exchanges; Morale, Welfare

and Recreation organizations; Non-Appropriated Fund organizations; and educational entities such as National Defense University) typically operate networks that may not be part of the DISN (i.e., do not use DISN transport or NIPRNet services such as internet access via the NIPRNet IAPs) or .mil domain. These Mission Partners and their networks may be in the gov/.org/.com/.edu domains and may be accessed directly from the internet through a boundary such as a DOD IAP that they operate and authorize or a contracted third-party DHS/GSA trusted internet connection (TIC). Such other networks and COI may interconnect with NIPRNet or SIPRNet and may interconnect with other DOD and non-DOD Mission Partner/Agency networks.

While the CAP concepts presented here are applicable to non-native DISN networks operated by other DOD components (e.g., the .edu community, which supports a diverse non-DOD user base), other methods may also protect these networks from risks associated with the use of commercial cloud. The use of a cloud access security broker (CASB) service with at least a FedRAMP Moderate PA might be one such alternative for non-DISN networks.

MPEs that use networks other than NIPRNet or SIPRNet (e.g., DRSN) will need to implement BCAPs or ICAPs for networks that provide protections equivalent to those defined in the SCCA FRD when connecting CSP infrastructure to their networks. MPEs implemented as a COI overlay on NIPRNet or SIPRNet can use the DISA-provided CAPs to fulfill the CAP requirement or may provide their own CAP capability in accordance with the SCCA. Mission Partners that are external to NIPRNet or SIPRNet are responsible for providing an equivalent capability to protect DOD data and MPEs from vulnerabilities associated with a connection to an external service provider.

All MPE CAP instantiations must be approved by the DOD CIO. MPE network connectivity/access to off-premises commercial DOD Level 4/5 CSOs will not traverse a NIPRNet BCAP or a NIPRNet Federated Gateway (NFG) when connecting to/accessing MPE applications instantiated in such a CSO.

5.9.1.6 Mission Partner Environment Access to NIPRNet Services Hosted in the Cloud

MPEs that require access to NIPRNet services are required to connect to NIPRNet via the internet, IAPs, and DOD DMZ or via an NFG in accordance with JFHQ-DODIN TASKORD 16-0103: Establishment of the NIPRNet Federated Gateway (NFG).

NIPRNet services are applications operated by DOD components to serve NIPRNet users. Some of these NIPRNet-focused applications might be implemented in a CSO. This might be a commercial off-premises CSO, a DOD private off-premises CSO, or a DOD private on-premises CSO. Mission Partners that desire or require access to such applications must coordinate with the Mission Owner of the application for permission to access it and to determine the best access method. Following are the three approved methods of accessing such an application:

- The MPE user must establish a VPN connection to NIPRNet or the application itself.
- The Mission Owner must expose the application to the internet through the DOD DMZ such that the MPE user can access the application from the internet via the IAPs.
- The Mission Owner must expose the application to the MPE network and MPE users through the NFG.

5.9.1.7 Mission System Connection Approval through DISN BCAPs

Impact Levels 4/5: Connection of a mission system to the DISN via an ICAP or BCAP will be approved and recorded by the DISA Connection Approval Office in accordance with normal connection approval procedures. This requires all Mission Owners to register all cloud-based applications, their CSP/CSO, and connection method in the DISA Systems/Network Approval Process (SNAP) database Cloud Module. Initial connections (physical or virtual) to a CSP's network will occur during onboarding of the CSP's first Mission Owner customer. Additional connections will be made, or capacity will be scaled, as more Mission Owners use the given CSP. Specific processes and procedures regarding connection approval and Mission Owner connections via a BCAP are addressed in the DISA Cloud Connection Process Guide (CCPG), which will ultimately be merged with the overall DISN Connection Process Guide (CPG).

Impact Level 6: The DOD Mission Owner systems/applications instantiated in these Impact Level 6 CSO enclaves will be assessed and authorized in the same way as any other DOD SIPRNet enclave connection in accordance with the DISA CPG. Approval for connection to the SIPRNet will be processed through the DISA classified connection approval process as with any other SIPRNet enclave.

5.9.1.8 Cloud Native Access Point (CNAP)

CNAPs are discussed in the DOD Cloud Native Access Point Reference Design document:

- https://DODcio.defense.gov/Portals/0/Documents/Library/CNAP_RefDesign_v1.0.pdf

5.9.2 Network Planes

A plane, in a networking context, is one of three integral components of network architectures. These three elements – the data synchronization/control or network plane, the user/data or production plane, and the management plane – can be thought of as different areas of operations. Each plane carries a different type of traffic and is conceptually an overlay network on top of the network plane.

5.9.2.1 Network Plane Connectivity

The network or data sync/control plane carries signaling traffic and data replication between servers/data centers. Network control packets originate from or are destined for a network transport device (virtual or physical). The network plane in general is subject to network-related DOD SRGs and STIGs. This Cloud Service Provider SRG does not contain additional requirements related to network plane connections to the cloud computing infrastructure.

5.9.2.2 User/Data Plane Connectivity

The user/data plane (also known as the forwarding plane, carrier plane, or bearer plane) carries the network user traffic. Table 5-1 details the DOD user/data plane connectivity by Impact Level for DOD on-premises and off-premises CSOs.

This table applies to non-DOD federal government tenants using a DOD on-premises CSO but does not apply to non-DOD federal government tenants using an off-premises CSO that is a federal government community cloud having DOD tenants.

Table 5-1: User/Data Plane Connectivity

Impact Level	Off-Premises Non-DOD CSP Service Offering Infrastructure	On-Premises DOD and Non-DOD CSP Service Offering Infrastructure
Level 2	• User connectivity will leverage commercial infrastructure (i.e., internet). • Users connecting from the internet will connect directly and users connecting from inside the DISN (i.e., NIPRNet) will connect to the internet via the DISN IAPs and then to the CSP infrastructure. • CSO connections will be assessed and authorized using the same external connection requirements as any other internet-facing connection.	• User connectivity will use existing infrastructure (government owned) for its user/data plane when the user is within the B/P/C/S fence line (on-premises) and directly connected to the local Base Area Network (BAN) and NIPRNet. • User traffic to/from the NIPRNet to/from the CSO infrastructure will traverse an ICAP. When the user is outside the B/P/C/S fence line (off-premises) connected to the internet, user traffic must enter/leave the NIPRNet via the DISN IAPs and then an ICAP. • CSO connections will be assessed and authorized the same as any other internal connection.
Level 4 and 5	• DOD and external user connectivity will leverage a DISN extension to the commercial facility using government network infrastructure within government boundaries (i.e., NIPRNet) and commercial infrastructure beyond government boundaries (i.e., commercial carrier infrastructure/connectivity service offerings). • The DISN extension will traverse a BCAP. • Users connecting from inside the DISN (i.e., NIPRNet) will connect via a BCAP, and users connecting from the internet will traverse the IAPs and then a BCAP. CSO connections will be assessed and authorized through the Connection Approval Process the same as any other internal connection and using the same requirements as any other DOD-facing or internet-facing connection.	

Impact Level	Off-Premises Non-DOD CSP Service Offering Infrastructure	On-Premises DOD and Non-DOD CSP Service Offering Infrastructure
Level 6	• User connectivity will leverage a DISN extension to the commercial facility using government SECRET network infrastructure within government boundaries (i.e., SIPRNet) and commercial infrastructure beyond government boundaries (i.e., commercial carrier infrastructure/connectivity service offerings). • The DISN extension to a commercial facility can be accomplished with a Multiprotocol Label Switching (MPLS) router and optical switch (referred to as a Service Delivery Node). • The DISN extension to a commercial facility will use the Commercial National Security Algorithm (CNSA) suite cryptography algorithms and key sizes. • User traffic to/from the internet (e.g., executive travel kits users) will use the CNSA suite and must enter/leave the SIPRNet via the approved gateways.	• User connectivity will use existing SECRET network infrastructure (government owned) for its user/data plane (i.e., SIPRNet). User traffic to/from the SIPRNet will traverse an ICAP. • User traffic to/from the internet (e.g., executive travel kits users) will use the CNSA suite cryptography algorithms and key sizes and must enter/leave the SIPRNet via the approved gateways. • CSO connections will be assessed and authorized the same as any other internal connection using the same requirements as any other SIPRNet - facing connection.

5.9.2.3 Management Plane Connectivity

The management plane carries network/server/system privileged user (administrator) traffic along with maintenance and monitoring traffic.

Table 5-2 details the management plane connectivity by Impact Level for a Mission Owner's systems/applications and CSP's CSOs. The Mission Owner management plane includes connectivity for DOD personnel or DOD contractors managing Mission Owner systems (i.e., virtual machines and networks) instantiated on IaaS/PaaS as well as for DOD personnel or DOD contractors' access to/use of CSP service ordering/management portals for all service offering types (IaaS/PaaS/SaaS). The CSP management plane includes connectivity for CSP personnel managing the CSP's service offering infrastructure.

All encryption identified, except as stated otherwise, must be accomplished using FIPS 140-2 or FIPS 140-3 validated cryptography modules operated in FIPS mode.

In accordance with standard practice and security requirements, management interfaces on virtual machines and protective appliances (virtual or physical) located in a Mission Owner's virtual

network must not be exposed to direct access from the production network (e.g., internet or NIPRNet/SIPRNet). To the extent possible, CSP service ordering/management portals through which virtual machines and virtual networks are instantiated and configured must also be protected from direct access from the production network to prevent compromise of mission systems and DOD information.

All management transactions must be audited.

Table 5-2: Management Plane Connectivity

Impact Level	Mission Owner Management Plane	CSP Management Plane
Level 2	• **Management connectivity from outside the NIPRNet** (e.g., for off-premises contractor personnel) requires an encrypted, tunneled connection via the internet to the mission system/application and virtual network. Management traffic to CSP service ordering/service management portals must be encrypted if not in an encrypted VPN. Monitoring traffic must traverse a VPN connection. All traffic entering/leaving the NIPRNet must be via the DISN IAPs. • **Management connectivity from inside the NIPRNet** (e.g., for on-premises DOD or contractor personnel) must be restricted to a defined set of IP addresses and requires an encrypted, tunneled connection through the NIPRNet to the internet via the IAPs to manage the mission system/application and virtual network. Management traffic to CSP service ordering/service management portals must be encrypted if outside an encrypted VPN. Monitoring traffic must traverse a VPN connection. All traffic must enter/leave the NIPRNet via the DISN IAPs.	• **Non-DOD CSP off-premises service offering infrastructure and off-premises management:** CSP management connectivity leverages CSP service offering and management plane infrastructure, which should be logically or physically separate from production. DOD cannot dictate how a CSP architects its commercial service offerings that are not dedicated to DOD. DOD recommends logical or physical separation of service offering production and management plane infrastructure as a well-known industry best practice. Such separation will be assessed as a bullet point for DOD risk acceptance. • **Non-DOD CSP on-premises service offering infrastructure and management:** The CSP may directly connect its management infrastructure to its service offering infrastructure if collocated. An encrypted, tunneled connection from the CSP's on-premises management infrastructure to the service provider's on-premises service offering infrastructure is also permitted locally but must be used to access remote service offering infrastructure. • **Non-DOD CSP on-premises service offering infrastructure and off-premises management:** CSP management connectivity must
Level 4 And 5	• **Management connectivity from inside the NIPRNet** must be restricted to a defined set of IP addresses and requires an encrypted, tunneled connection through the NIPRNet and an ICAP or BCAP to	

Impact Level	Mission Owner Management Plane	CSP Management Plane
	manage the mission system/application and virtual network. Management traffic to CSP service ordering/service management portals must be encrypted if not in an encrypted VPN. Monitoring traffic must traverse a VPN connection. All traffic must enter/leave the NIPRNet via a BCAP. • **Management connectivity by DOD personnel or DOD contractors from outside the NIPRNet** must be restricted to a defined set of IP addresses and requires an encrypted, tunneled connection from the internet via an IAP and an ICAP or BCAP to the mission system/application and virtual network. Per remote administration policy, the remote management terminal must be GFE. Management traffic to CSP service ordering/service management portals must be encrypted if outside an encrypted VPN. Monitoring traffic must traverse a VPN connection via a BCAP and NIPRNet.	leverage an encrypted, tunneled connection from the CSP's off-premises management infrastructure to the service provider's on-premises service offering infrastructure. • **DOD CSP on-premises service offering infrastructure and management:** CSP management connectivity will use existing infrastructure such as the Enterprise Services Directorate (ESD) out-of-band (OOB) management network. No service provider security stack is required.
Level 6	• All management and monitoring connectivity is executed via the SIPRNet. Management and monitoring traffic will be encrypted using FIPS 140-2 or FIPS 140-3 validated cryptography to accommodate separation for need-to-know reasons.	• **DOD CSP on-premises service offering infrastructure and management:** CSP management connectivity will use existing SECRET network infrastructure such as the SECRET OOB management network. No service provider security stack is required. • **Non-DOD CSP on-premises service offering infrastructure and management:** The CSP may directly connect its management infrastructure to its service offering infrastructure if personnel are collocated using their SECRET LAN. An encrypted, tunneled connection using FIPS 140-2 or FIPS 140-3 validated cryptography over SIPRNet from the CSP's on-

Impact Level	Mission Owner Management Plane	CSP Management Plane
		premises management infrastructure to the service provider's on-premises service offering infrastructure is also permitted and will be used to access remote service offering infrastructure. • **Non-DOD CSP on-premises service offering infrastructure and off-premises management:** CSP management connectivity must leverage a SIPRNet extension or a DOD-approved encrypted, tunneled connection from the CSP's dedicated SECRET off-premises management infrastructure to the service provider's on-premises service offering infrastructure. • **Non-DOD CSP off-premises service offering infrastructure and off-premises management:** CSP management connectivity leverages CSP's dedicated SECRET service offering and management plane infrastructure, which must be logically or physically separate.

5.9.3 CSP Service Architecture

DOD uses the concept of defense-in-depth when protecting its networks and data/information. This includes but is not limited to hardening host operating systems and applications, implementing host firewalls and intrusion detection, strong access control, and robust event auditing, while protecting the networks with application layer firewalls, proxies, web content filters, email gateways, intrusion detection/prevention, and a DMZ/gateway architecture, along with robust network traffic monitoring. The concept must not be lost when moving Mission Owners' systems/applications and their data/information to the commercial cloud. If virtualization is used, the above measures must also be used to protect the virtual environment along with the use of hypervisor-based firewall/filtering/routing mechanisms or virtual security appliances.

This section details the defense-in-depth security concepts and requirements that both CSPs and Mission Owners must implement to protect DOD data/information and mission systems/applications. DOD recognizes that innovative approaches can be implemented in the virtual environment that may replace some of the defense-in-depth mitigations developed for physical networks and servers. DOD looks forward to evaluating equivalent alternative measures, which DISA will assess on a case-by-case basis.

5.9.3.1 CSP Service Architecture – SaaS

Mission Owner use of a CSP's SaaS offerings relies on the defense-in-depth measures implemented by the CSP for the protection of the service application and the infrastructure that supports it. This includes the protection of all sensitive information stored and processed in the CSP infrastructure. In other words, the Mission Owner relies on the CSP and the security posture of its SaaS offering for the protection of DOD information. During the ATO assessment process for SaaS offerings, defense-in-depth security/protective measures must be assessed for adequacy and potential risk acceptance by DOD. This may be in addition to assessing security controls. The following guidance is reflected in the Application Security and Development STIG and other operating system and application-specific STIGs but is highlighted here to emphasize instances where an authoritative reference (e.g., product-specific STIG) is not available.

Due to the normal internet connectivity for CSOs, DOD expects the CSP to establish defense-in-depth security/protective measures for P/SaaS CSOs where the Mission Owner does not have control of their infrastructure environment. These measures include but are not limited to the following:

- Properly configured application layer and web application firewall(s), intrusion detection and/or prevention protection of the CSP's infrastructure supporting the SaaS application offering, and segmentation (logical or physical) from the CSP's other offerings and corporate networks.
- Application/network tiered architecture that provides "front end" unrestricted/restricted DMZ zones with appropriate protections for internet/externally facing servers and private/"back end" zones with appropriate protections for application/database servers and other supporting systems/servers. This includes but is not limited to web application firewalls, reverse web proxies, and FTP proxies as necessary to protect the application and the customer's data/information stored/processed within.

  PaaS/SaaS CSOs where the Mission Owner does not have control of their infrastructure environment typically serve NIPRNet users and thus are NIPRNet facing via the BCAP. Some Mission Owners need a portion of their CSO application to be internet facing. In such cases, the internet-/NIPRNet-facing portion of the application must use a separate web server(s) and IP address(es) from those only facing the NIPRNet so they can be allowlisted for access via the IAPs and protect the NIPRNet facing web server(s).

  The internet-facing IP addresses will also be available for access from the NIPRNet.
- Customer data-at-rest encryption protections using FIPS 140-2 or FIPS 140-3 validated cryptographic modules operated in FIPS mode where only the Mission Owner has control of the keys. This requirement addresses the persistent storage of customer data on various media and in databases, not customer data that requires real-time processing without retention. If such data is retained, the retained data storage is persistent.
- Customer data-in-transit encryption protections using FIPS 140-2 or FIPS 140-3 validated cryptographic modules operated in FIPS mode. This requirement addresses customer data transiting public and private wide area networks (WANs) such as the internet, NIPRNet, and the CSP's WAN, and local area networks (LANs) from the customer terminal to the CSP's service offering enclave LAN. Encryption may be native at the protocol level or be at the VPN/tunnel level. This requirement also applies to CSP replication of customer data and systems between primary locations and backup continuity of operations (COOP)/disaster recovery (DR) locations.

- Hardening/patching/maintenance of operating systems and applications in accordance with industry standards. DOD SRGs and STIGS must be used if the service is a private or community cloud used by DOD. For Information Assurance (IA) Vulnerability Management (IAVM) message compliance, the CSP will be expected to comply with industry best practice by applying patches identified in the Common Vulnerabilities and Exposures (CVE) that would be referenced in the DOD IAVM message. Innovative alternatives such as implementing a behavioral-based or software integrity protection model for all systems may be viable and will be assessed on a case-by-case basis.
- Implement PIV/DOD CAC/PKI authentication for all customer user access on all SaaS offerings that process information at Impact Levels 4 and 5 in accordance with IA-2 (12). This includes regular nonprivileged users accessing the service and privileged customer users accessing service ordering/management interfaces/portals. SaaS offerings that process information at Impact Level 6 must use the CNSS SIPRNet token. Alternate authentication measures for user communities that cannot use the required PKI token will be assessed on a case-by-case basis and may require a waiver.

5.9.3.2 CSP Service Architecture – IaaS/PaaS

Mission Owners build systems and applications on virtualized infrastructure provided by the CSO under IaaS/PaaS. Responsibility for security must be clearly delineated between the CSP and the Mission Owner, depending on how the CSP presents the security features it supports in the CSO. Under IaaS, the Mission Owner is fully responsible for securing the guest operating systems and applications that they build; the CSP will be responsible for securing the virtualization operating system (i.e., hypervisor) and supporting infrastructure.

Under PaaS, the Mission Owner is fully responsible for securing the guest operating systems and the platform applications and applications that they build. Depending on how the CSP CSO presents the security features it supports in the CSO, the delineation of responsibility may partially shift from the Mission Owner to the CSP with respect to the guest operating systems and the platform applications. The CSP might take responsibility for securing these areas of a PaaS CSO as part of the core service or as an add-on component.

IaaS and PaaS offerings are generally treated the same, with the Mission Owner responsible for securing the operating system and platform applications. Mission Owners must assess inherited mitigations that the CSP provides to determine that defense-in-depth security/protective requirements are fully met.

CSP IaaS and PaaS offerings must support the defense-in-depth security/protective measures that the Mission Owner must implement to secure the systems and applications they build on the service offering.

5.9.3.3 CSP Disaster Recovery (DR) – Continuity of Operations (COOP)

As a best business practice, CSPs plan for DR and COOP and implement infrastructures to support these contingency plans. This typically includes geographically separate facilities/data centers. FedRAMP also assesses several security controls related to contingency planning (i.e., DR and COOP).

Data replication between a CSP's geographically separate facilities/data centers is typically required for DR and/or COOP. This includes data backup.

All data replications must traverse a CSP's private internal network (physical or virtual) from CSP offering site/location to the DR/COOP facility and protect the data in transit. If this network traverses the internet, the network connection must be encrypted end-to-end in an IPsec tunnel implemented using FIPS 140-2 or FIPS 140-3 validated cryptography. Separation requirements implemented in the CSO between DOD data and non-DOD data at the CSP offering site/location must be replicated at the DR/COOP facility. Such separation is not specifically required in transit unless its implementation is required to support separation at the endpoint facilities.

For Impact Level 4/5 CSOs, such transfers do not route through the DISN BCAP unless the DR/COOP facility is on-premises or is another CSP's CSO.

Related Controls: CP-6, CP-7, CP-9.

5.9.4 Internet Protocol (IP) Addressing and Domain Name Services (DNS)

DOD is required to conduct DOD public and private internet-based communications (e.g., electronic mail and web operations) under the top-level domain (TLD) names established for the DOD—the .mil TLD. Exceptions are provided for some DOD organizations, which may use the .gov, .edu, and .com domains if necessary and approved by the Mission Owner's CIO. This means the end user accessing a DOD website or other resource using a URL will see ".mil" at the end of the URL (e.g., name.mil is required versus name.com).

DOD IP addresses are to be used only on DOD systems located on or connected to as an extension of the NIPRNet or SIPRNet.

A .mil URL not redirected to non-.mil domain named hosts (e.g., name.mil will not redirect to name.com). The only exception is for an approved and accredited service that provides redirection not readily apparent to the end user (e.g., use of a content delivery service or cloud service). This exception permits the use of a canonical name (CNAME) in the system's DNS record within the DOD DNS servers that redirects the URL to the CSP-assigned URL associated with the commercial IP address. The end user must not be made readily aware of the redirection.

The example of electronic mail (email) in DODI 8410.01 paragraph 3a and previously in this section does not negate the use of an external commercial cloud email service by DOD components, providing the URL to access the service ends in ".mil" and the redirection is not readily apparent to the user.

IP addresses assigned by ARIN to the DOD NIC, which are then assigned to DOD components for their networks and information systems (e.g., NIPRNet addresses), are unique publicly routable addresses. RFC 1918 addresses are "private" (non-publicly routable) which are permitted/used within DOD network enclaves and within CSO enclaves behind the external publicly routable addresses.

5.9.4.1 Off-Premises IP Addressing

5.9.4.1.1 Off-Premises Impact Level 2 IaaS/PaaS/SaaS

Due to off-premises Impact Level 2 IaaS/PaaS/SaaS CSOs being directly accessed from the internet, DOD Mission Owner systems/applications using the .mil domain that are implemented in an Impact Level 2 IaaS, PaaS, or SaaS CSO where the Mission Owner has control over their IP addressing will be addressed using public IP addresses assigned and managed by the CSP. This also applies to DOD Mission Owner systems/applications approved to use non-.mil domain names. In this case, the DOD DNS server will use a CNAME for a .mil URL to point to the commercial URL and its IP address. Similarly, PaaS or SaaS CSOs where the Mission Owner does not have control over the IP addressing will be managed using public IP addresses assigned and managed by the CSP.

The use of "private" RFC 1918 IP addresses internal to the virtual network enclave with commercial addresses on the internet-facing interfaces is acceptable and is recommended minimally for topology hiding.

5.9.4.1.2 Off-Premises Impact Level 4/5

DOD IP addresses are assigned/managed by the DOD NIC and may be further managed and assigned to networks and information systems by DOD component NICs. NIPRNet, subtended Component enclave networks, and their internally connected endpoints must be addressed using DOD NIPRNet IP addresses.

The following is NOT applicable to DOD systems that are not connected to, or not part of, the NIPRNet and are already approved to use non-DOD, non-NIPRNet IP addresses. There is no intent to force such DOD systems to become part of the NIPRNet.

Mission Owners' systems/applications instantiated in IaaS and in some PaaS CSOs have full control over the IP addressing of their systems/applications instantiated in the CSO, and because they are connected to NIPRNet through a NIPRNet BCAP, DOD NIPRNet IP addresses will be used. This also applies to SaaS and PaaS where the Mission Owner has control over the IP addressing used in their portion of the CSO. These systems/applications are within a network enclave that is considered an extension of the NIPRNet. The DOD NIC has set aside a range of NIPRNet IP addresses for CSOs connected to the NIPRNet BCAP. Mission Owners/CSO sponsors may make IP address requests through the DOD NIC website. This requirement applies similarly to networks other than NIPRNet where a BCAP is required. In such cases, IP addresses used on that network will be used.

As with any DOD enclave, the use of "private" RFC 1918 IP addresses internal to the virtual network enclave with NIPRNet addresses on the NIPRNet/internet-facing interfaces connected via the BCAP is acceptable.

DOD's objective requirement for all off-premises Level 4/5 CSP's PaaS and SaaS CSOs serving the DOD, where the Mission Owner does not have control over IP addressing, is for the CSO to offer a "bring your own" IP address capability for all customer-facing interfaces so that DOD NIPRNet IP addresses may be used and accessed via the private connection and BCAP. In this case, customer-facing interfaces include general user interfaces and customer management interfaces including CSO

customer service management/ordering portals. DOD does not want to be required to access such portals via the internet except during initial setup of the CSO.

This IP addressing requirement does not include CSP systems instantiated within the CSO infrastructure that are not customer facing or directly accessible from the NIPRNet (or other Mission Partner network). Such internal systems and infrastructure may use IP addresses assigned and managed by the CSP.

If a Mission Owner's application in I/PaaS where they have control of the addressing, or the P/SaaS CSO where they do not have control of the addressing, must face both NIPRNet and internet via the BCAP, separate IP ranges must be assigned to the NIPRNet-only facing servers from those assigned to servers available from NIPRNet and the internet. This is to facilitate registering the internet-facing IP addresses as DOD DMZ addresses and adding them to the DOD DMZ/IAP allowlist while protecting the NIPRNet-facing servers from internet threats.

5.9.4.1.3 Off-Premises Impact Level 4/5 Commercial IP Addressing and Routing for SaaS and Some PaaS

DOD recognizes that with some off-premises commercial SaaS and PaaS CSOs today, it is not possible or practical for the CSO to support customer IP addressing for several reasons. In such cases, the Mission Owner will not have control over the IP addressing of the CSO as would be the case with a "bring your own" IP address capability. Therefore, CSP-managed commercial IP addresses must be used and interfaced with the NIPRNet via the BCAP. DOD's preferred solution is for the CSP to provide a Network Address Translation (NAT) or proxy between the CSO and NIPRNet BCAP so that NIPRNet need only route DOD IP addresses.

Alternate solutions that require a CSO's commercial IP addresses to be routed on the NIPRNet must be assessed and approved through a non-DOD addressing risk assessment and risk acceptance process. This may affect the ability of the CSO to be awarded a DOD PA or may result in a PA with conditions. The CSP must work and coordinate with DISA to achieve such an alternate solution to minimize the operational and cybersecurity effects on the DISN/NIPRNet.

The following is a set of minimum constraints and requirements that will be considered for the non-DOD addressing risk acceptance/PA conditions and must be adhered to for ongoing operations:

- Vendors must provide a complete list of their commercial IP subnets that need to be routed on NIPRNet to affect such routing.
  - These route advertisements must be aggregated to /24 or larger blocks in support of current DISN capabilities.
  - Although changes are to be expected over time, the frequency of changes to the list must be minimal to decrease the management burden on DISA operators and reduce network service disruptions.
- Commercial IP subnets advertised to NIPRNet via the BCAP used to access DOD services and applications in off-premises CSOs must be dedicated to DOD and separate from the IP addresses used to access the CSO from the internet.
- Commercial IP subnets advertised to NIPRNet via the BCAP used to access DOD services and applications in off-premises CSOs must not also be advertised to the internet from the

CSP's infrastructure. If they are, they must not be reachable from the internet (i.e., Impact Level 4/5 DOD accounts, services, and applications which, per DOD policy, are only to be accessible from the NIPRNet must not be accessible directly from the internet). This means the same IP addresses must not be used for accessing the CSO from the NIPRNet that are used for accessing it from the internet. This will cause routing issues for both parties.

- If a Mission Owner's application in P/SaaS CSO where the Mission Owner does not have control of the addressing must face both NIPRNet and internet via the BCAP, separate IP ranges must be assigned to the NIPRNet-only facing servers from those assigned to servers available from NIPRNet and the internet. This is to facilitate registering the internet-facing IP addresses as DOD DMZ addresses and adding them to the DOD DMZ/IAP allowlist while protecting the NIPRNet-facing servers from internet threats.
- DOD expects the CSO's commercial IP addresses used to access Impact Level 4/5 DOD accounts, services, and applications in the CSO via the BCAP and private connection to be dedicated for DOD NIPRNet user access. However, if the CSO must use the same IP addresses for access by all CSP/CSO customers, whether DOD or non-DOD (this assumes the non-DOD customer access is via the internet), the CSP must take extra precautions to prevent the CSO's internet connection or a compromised system from becoming a back door to the NIPRNet. The CSP must also ensure that direct traffic to the CSO from the internet is not potentially routed over NIPRNet.
- DISA will NOT advertise any CSP's commercial IP subnets used for both direct internet access and NIPRNet to the internet via the NIPRNet IAPs. Doing so could cause unauthorized traffic to the CSO from the internet to attempt to traverse the NIPRNet. DISA cannot support such traffic for both operational and cybersecurity reasons. Only DOD IP addresses associated with .mil URLs or a CSO's DOD dedicated commercial IP addresses accepted as routable on NIPRNet may be advertised to the internet via the IAPs.
- If a Mission Owner implements a "cloud" VPN between the BCAP and their intranet gateway/boundary for a CSO that is also used by other Mission Owners, the same commercial IP addresses may be visible and reachable from the NIPRNet, internet, and Mission Owner's intranet. In this case, the Mission Owner is responsible for controlling their own routing policies. The Mission Owner must implement routing and security policies within their network to enforce service access control during both normal and failure scenarios.

5.9.4.1.4 Off-Premises Impact Level 6

All off-premises CSP's Level 6 CSOs will be treated, designed, and addressed as an extension of the SIPRNet (i.e., a SIPRNet network enclave) or other SECRET Mission Partner network.

All Mission Owner systems/applications instantiated in IaaS/PaaS (i.e., virtual machines and virtual network device interfaces) and connected to SIPRNet will be addressed using SIPRNet IP addresses. This includes management plane systems and interfaces.

All off-premises CSP Level 6 SaaS and some PaaS service offerings connected to SIPRNet must use DOD assigned and managed SIPRNet IP addresses throughout. Alternate internal addressing will require a waiver.

5.9.4.2 On-Premises IP Addressing

5.9.4.2.1 IP Addressing for On-Premises Impact Level 2/4/5

All on-premises Impact Level 2/4/5 IaaS/PaaS/SaaS CSOs and Mission Owner systems/applications will be addressed using DOD NIPRNet IP addresses.

5.9.4.2.2 IP Addressing for On-Premises Impact Level 6

All on-premises Impact Level 6 IaaS/PaaS/SaaS CSOs and Mission Owner systems/applications will be addressed using DOD SIPRNet IP addresses.

5.9.4.3 Domain Name Services (DNS)

DOD .mil DNS servers on NIPRNet (and .smil.mil DNS servers on SIPRNet) are authoritative for DOD IP addresses provided through the DOD NIC and subtended Component NICs. This means that the DOD .mil DNS servers resolve .mil URLs to their destination IP address. DOD .mil DNS servers on NIPRNet must also be used to host .mil URLs that cannot have a specific IP address associated with them. In this case, a CNAME is used in the DOD .mil DNS servers on NIPRNet to point to a commercial URL used by the CSO.

DOD .mil DNS servers on NIPRNet are protected using various security measures such as the DOD DNS proxies, the Enterprise Recursive service, and DNSSEC. DOD DNS is protected from many DNS threats, and DOD DNS and associated protective services must be used for DOD .mil URLs and address resolution as appropriate.

5.9.4.3.1 On-Premises and Off-Premises Impact Level 2/4/5

In general, Mission Owner systems/applications using the .mil domain instantiated in an IaaS/PaaS/SaaS CSO, where the Mission Owner has control over the IP addressing and is using DOD NIPRNet IP addresses, must host .mil DNS records in the DOD .mil NIPRNet authoritative DNS servers and not in public or commercial DNS servers. Therefore, such Mission Owners are not authorized to use DNS services offered by the CSP or any other non-DOD DNS provider unless otherwise approved to use another domain. Mission Owners using non-.mil URLs may use CSP-managed or other commercial/public DNS servers (not the DOD DNS servers) for the domains in which they are authorized to operate.

Exception for Off-Premises Impact Level 2: DOD Mission Owners using an off-premises Impact Level 2 CSO, which by default uses CSP-managed commercial IP addresses and URLs, must host .mil DNS records in the DOD .mil NIPRNet DNS servers and use a CNAME to point to the commercial URL or IP address as appropriate. CSP DNS servers will be authoritative for commercial IP address resolution.

Exception for Off-Premises Impact Levels 4/5 SaaS and Some PaaS: DOD Mission Owners using an off-premises Impact Level 4/5 CSO (IaaS and some PaaS), where the Mission Owner does not have control over the IP addressing and therefore depends on CSP-managed commercial IP addresses and URLs, must host .mil DNS records in the DOD .mil NIPRNet DNS servers and use a CNAME to point to the commercial URL for IP address resolution as appropriate. CSP DNS

servers will be authoritative for their commercial IP address resolution. If use is required, CSP DNS services including URL redirection and dynamic DNS solutions, along with implemented DNS protections, will be assessed and approved as appropriate for the CSO's DOD PA. CSP DNS services must be protected using a DNS proxy and must support DNSSEC. The DOD PA will also include a risk assessment of the CSP's DNS management architecture or outsourced services.

All On-Premises and Off-Premises Impact Level 6: DOD Mission Owners using an on-premises or off-premises Impact Level 6 CSO will use smil.mil URLs whose DNS records will be hosted on the DOD authoritative DNS servers on the SIPRNet (or other SECRET Mission Partner network). SIPRNet addresses are assigned by the DOD NIC.

Corresponding Security Controls: SC-20, SC-21, SC-22.

5.9.5 Hybrid Cloud – Interconnections Between CSOs

In the interconnection of a higher Impact Level CSO with a lower Impact Level CSO, the transfer of the higher impact information to the lower Impact Level CSO must be prevented unless an approved cross-domain solution (CDS) is used and appropriate approval procedures are followed.

5.9.5.1 Mission Owners' Applications

Mission Owners may need to leverage multiple off-premises CSOs for various reasons. For Impact Level 4/5 or Impact Level 6 CSOs, the interconnection of these CSOs must be monitored so that unauthorized traffic and information transfer is avoided and audited.

- Connections between CSOs from the same CSP will remain on the CSP's network.
- Connections between CSOs from different CSPs will traverse the CSO's connections to the meet-me router(s). While not desirable due to circuit capacity usage concerns, some traffic might be routed through the BCAP if deemed necessary.

In all cases, the interconnected CSOs will audit traffic. Some auditing may occur at the meet-me router (or BCAP) for connections that traverse these points.

5.9.5.2 On/Off-Premises Scenarios

Mission Owners may need to leverage multiple Impact Level 4/5 or Impact Level 6 CSOs that are both on-premises and off-premises. The interconnection of these CSOs will be via the BCAP.

5.9.5.3 SaaS CSOs Using "External Services"

A commercial CSP, to provide a complete SaaS CSO, may leverage one or more third-party "external services." These may include notification services, scanning and audit services, and/or others. CSOs seeking an Impact Level 4/5 PA must ensure that sensitive DOD data is not transmitted to, or via, such external services unless that service has a DOD PA or is addressed in the CSO's PA. If the CSO is an Impact Level 4/5 CSO, traffic to and from such services will not traverse the DISN BCAP, assuming the CSO serves non-DOD customers. The CSP must ensure

that such external service connections, likely to be via the internet, do not permit access to NIPRNet via the BCAP from such connections.

5.10 DOD Contractor/Component Mission Partner Use of CSOs

This section focuses specifically on non-CSP DOD contractors or Mission Partners (e.g., Defense Industrial Base [DIB] contractors) and DOD component Mission Partners (e.g., commissaries, exchanges, educational entities) whose networks are not part of the DODIN .mil domain. These Mission Partners and their networks are typically in the .gov, .org, .com, and .edu domains.

When using cloud services, Mission Partners and contractors are responsible for following all guidance in this Cloud Service Provider SRG related to the Mission Owner that is not specific to a DISN-provided capability (e.g., CAP) or an enterprise service. The appropriate Impact Level must be selected based on the DOD data being processed. A trusted means of communication that encrypts all DOD data transferred between Mission Partners and contractor internal networks and CSPs must be used. Mission partners and contractors are also responsible for working with the appropriate DOD data owner or designated agency (e.g., DCSA) to create incident response procedures for incidents that occur in a CSO.

The term "non-CSP DOD contractors" as used below does not include DOD contractors that are not a CSP but aggregate CSOs (i.e., integrators) in the fulfillment of a contract for cloud services. As noted elsewhere in this Cloud Service Provider SRG, the CSOs these non-CSP integrators are providing via subcontracts must follow all guidance related to CSOs and DOD's use of them. For IaaS/PaaS, if a separate contractor (not the CSP) is brought into an already contracted space to make changes to, manage, or enhance that space, the new contactor is acting for the Mission Owner and must follow all guidance for Mission Owner personnel.

5.10.1 DOD component Mission Partners

DOD component Mission Partners in the .gov, .org, .com, .edu domains must only use CSPs or CSOs that have a DOD PA for the information Impact Level that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSP/CSO. If the information is public, a Level 2 CSO will be used with direct internet access. Otherwise, accessing Level 4/5 services depends on how their organizational network/enclave is connected today. This may be as follows.

The organizational network/enclave:

- Is part of NIPRNet; connectivity to the CSO will be via the NIPRNet BCAP.
- Is part of a Mission Partner or COI network with a BCAP; connectivity to the CSO will be via that BCAP.
- Is directly connected to the internet via one or more approved organizational IAPs; connectivity to the CSO will be via the internet or a private direct connection. Such connections will be appropriately secured for the protection of the organization's network and information/applications in the cloud. The organization's network boundary with the CSP's network will be considered a BCAP and will provide boundary protections and monitoring as required for the protection of the specific organization's network and

information it contains. DOD component Mission Partners are responsible for implementing appropriate boundary protections for their networks.

5.10.2 Non-CSP DOD Contractor's and DIB Partners' Use of CSOs to Protect Sensitive DOD Information

Non-CSP DOD contractors and DIB partners may store, process, and use or create sensitive DOD data/information outside of the DODIN in conjunction with a DOD contract not associated with providing cloud services. Such contractors are required to protect unclassified sensitive DOD data/information while it is in their environment (i.e., contractor owned/operated IT systems used by the contractor to support contractor functions that store DOD CUI).

Non-CSP DOD contractors and DIB partners may wish to use cloud services to fulfill their contract or protect/process DOD data they possess (i.e., CUI or CDI). Thus, for the protection of sensitive CUI/CDI, it is highly recommended that non-CSP DOD contractors use CSOs that have been granted a DOD Level 4 PA. Such CSOs must not be dedicated to DOD, which would mean the CSO is only connected to the NIPRNet. Access to the CSP/CSO will be via the internet or a private direct connection. The NIPRNet will not be used as a connection path. DOD contractors are responsible for implementing appropriate boundary protections for their networks and the protection of information placed in the cloud.

Non-CSP DOD contractors and DIB partners may NOT use CSOs that have been granted a DOD Level 5 PA because they are outside the supported community of federal agencies until such time as DOD changes this Level 5 limitation.

Non-CSP DOD contractors and DIB partners are required to comply with NIST SP 800-171 for the protection of CUI/CDI. The DOD Level 4 and Level 5 baselines cover all the security controls referenced in the SP 800-171 except CM-3(2), CM-7(4), and IR-2(1).

5.10.3 Non-CSP DOD Contractors Use of CSOs As a Portion of a Non-CSO Product or Service

A Non-CSP DOD contractor might choose to integrate a third-party CSO as a component of a contracted non-CSO product or service (e.g., a weapons system or major application). Such contractors may only use third-party CSPs or CSOs that have a DOD PA for the information Impact Level that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSP/CSO. The CSO and its use must follow the Cloud Service Provider SRG guidance related to the Mission Owner that is not specific to a DISN-provided capability (e.g., CAP) or an enterprise service to the greatest extent possible. Connectivity to the CSO will be determined by where the contracted product or service will be used and related guidance in this Cloud Service Provider SRG. For example, if the user base for the product or service is NIPRNet based and the information Impact Level is 4 or 5, the NIPRNet BCAP must be used. If the information Impact Level is 2, the internet may be used. All Cloud Service Provider SRG requirements apply to the product and flow down to the subcontracted CSO in accordance with various DFARS clauses.

If the non-CSP DOD contractor chooses to provide/host the CSO themselves, the Cloud Service Provider SRG requirements for the information Impact Level that best matches the CNSSI 1253 categorization of the information to be processed/stored/transmitted by the CSO applies. If the CSO is dedicated to the product, A&A will be handled in accordance with normal DOD contract A&A requirements. Consideration for awarding a DOD PA in this case will depend on the results of the A&A processes, compliance with the Cloud Service Provider SRG, and the potential for other DOD components' Mission Owners to use the CSO.

5.11 Mobile Code

While most of the compliance with DOD Mobile Code policy is the responsibility of the Mission Owner, SC-18 (2) states "The organization verifies that the acquisition, development, and use of mobile code to be deployed in information systems meets organization-defined mobile code requirements." Both CSPs and Mission Owners must comply with the DOD-specified values for the SC-18 control enhancements in Appendix D pertaining to an Impact Level 4/5/6 CSO. SC-18 (3) and SC-18 (4) have been assigned values. These are also included in the set of SLA controls to be added by Mission Owners for inclusion in the SLA/contract listed in the Cloud Computing Mission Owner SRG.

The CSP must enact similar mobile code policies for SC-18 (2). CSOs will prevent or be configurable to prevent the download of unapproved/risky mobile applications.

5.12 Supply Chain Risk Management Assessment

The DOD-selected FedRAMP baseline controls, SR family of controls, address Supply Chain Risk Management (SCRM). The acquisition of system components and software that are counterfeit, unreliable, or contain malicious logic or code is of great concern to DOD for all products supporting the processing, storage, and transmission of CUI and classified information. This concern extends to cloud computing.

As part of the CSO's DOD PA assessment package (if not already provided for the FedRAMP P-ATO or Agency ATO), the CSP will provide a SCRM plan outlining their supply chain assessment/management and component authenticity process and measures taken so they are not acquiring system components and software that are counterfeit, unreliable, or contain malicious logic or code and incorporating them into the CSO infrastructure or its management plane.

The CSP's SCRM plan for how the CSP implements the SR family controls will be assessed and approved during the DOD PA assessment process for all Impact Level 4, 5, and 6 CSOs.

5.13 Electronic Mail Protections

CSPs that operate/offer email servers/services must provide for appropriate email protections within the CSO. Mission Owners must use these services or provide for alternate capabilities when contracting for email services. Such protections will include but may not be limited to email hygiene or scanning for and elimination of malicious content and spam filtering as a minimum.

The Enterprise E-Mail Security Gateway (EEMSG) inspects all email inbound from, or outbound to, the internet. It further requires email outbound from one DOD component's email servers to another Component's email servers to pass through the EEMSG. The EEMSG only deals with server-to-server email traffic and not with client-to-server traffic. All DOD components are required to use the EEMSG as follows unless a waiver is in place. If a waiver is in place, the DOD component must use their own email security gateway.

- All email transfers inbound through the IAP from an external email server destined to an Impact Level 4/5 email server in a Mission Owner's enclave within a CSO via a BCAP must pass through the EEMSG inbound protections.
- All email transfers sent from an Impact Level 4/5 email server in a Mission Owner's enclave within a CSO via a BCAP and through the IAP to an external email server must pass through the EEMSG outbound protections.
- All email transfers sent from an Impact Level 4/5 email server in a Mission Owner's enclave within a CSO via a BCAP to email servers in a DOD component's data center enclave must pass through the EEMSG outbound protections.
- All email transfers sent from email servers in a DOD component's data center enclave to an Impact Level 4/5 email server in a Mission Owner's enclave within a CSO via a BCAP must pass through the EEMSG outbound protections.

This requirement is because the Mission Owner's environment in any CSO is considered a DOD enclave that may include an email server as the primary service SaaS offering or as an adjunct service to a PaaS/SaaS or may be instantiated by the Mission Owner in IaaS.

If two Mission Owners use the same email SaaS and email servers, there is no need for EEMSG protections for email between the different Mission Owners' users. However, if the CSO implements different servers/enclaves for different Mission Owners, the CSO must include an email hygiene/protective service through which email transfers between these servers/enclaves will route. In this case, the server-to-server email traffic will remain within the CSP's infrastructure and not traverse the CAP or EEMSG. Similarly, Mission Owners that implement email servers in IaaS or leverage a PaaS feature within their CSO-based enclaves will follow the same rules as above for SaaS and must provide for email hygiene/protective service within the CSO for traffic flowing between Mission Owner enclaves or route such traffic through the BCAP and EEMSG.

All BCAPs must support Mission Owners and implement the appropriate routing of server-to-server email traffic to/from the EEMSG capability at the CAP end of the connection for all CSOs that contain an email server. This includes routing to/from such servers and the IAP for email servers that are external and internet connected. This is a CSO connection approval requirement. However, it is ultimately a Mission Owner responsibility for TASKORD compliance when they use a CSO or implement a system/application in IaaS/PaaS.

As of this release of the Cloud Service Provider SRG, EEMSG does not inspect intra-enclave email. Therefore, the above requirements do not apply to email traffic that remains within the DISN and Mission Owner enclaves in a CSO, until EEMSG does inspect intra-enclave email. The requirement for EEMSG to inspect all email traffic to/from the internet-based email servers still applies.

5.14 Penetration Testing

The DOD will have the authority to perform internal and external penetration testing on all CSP IL6 hosting environments and service offerings at any time using DOD-approved methods in coordination with the CSP.

6. CYBERSPACE DEFENSE AND INCIDENT RESPONSE

Contracts, memorandums of agreement, support agreements, international agreements, or other applicable agreements must identify specific operations responsibilities, cybersecurity requirements, protection requirements for DOD data, and points of contact for mandatory reporting of security incidents.

An example of maintaining the security posture of a Mission Owner's system is the application of patches/upgrades and IAVM compliance. This is a Mission Owner requirement as identified by policy. However, in an SaaS environment, the operating system is managed by the CSP, and the CSP would be required to apply operating system patches.

6.1 Cyberspace Defense Actions

The following is a list of cyberspace defense actions and their responsibilities as they relate to cloud operations.

- **DODIN Cyberspace Defense (DCD) Actions:** The primary objective of the organization that performs DCD actions is to oversee a coordinated response to DODIN-wide attacks. DCD builds a broad picture of the operating environment across Mission Owners, MCDs, BCDs, CSOs, and CSPs. The DCD identifies patterns of incidents or events, consolidates related incident tickets, directs mitigations, and assigns DODIN Cyber Protection Teams (CPTs) to focus efforts on a specific threat or adversary. Specific cyberspace defense actions include:
  - Protect the DODIN and DOD mission systems in commercial cloud infrastructure through cross-BCAP correlation and analysis of events/data.
  - Direct or recommend cybersecurity actions regarding DODIN-wide incident and system health reporting involving a BCAP or CSP.
  - Establish and maintain external communications with the CSP for DODIN-wide incidents and ensure internal DOD communications are established between all entities, which include the MCD and BCD.
  - Interface with the U.S. Computer Emergency Readiness Team (US-CERT) to obtain relevant CSP information; ensure cross-sharing of information across all organizations performing BCD/MCD actions.
- **Boundary Cyberspace Defense (BCD) Actions:** The primary objective of organizations that perform BCD actions is to protect the DISN from events or incidents that use public, private, hybrid, or community clouds. BCD actions support CSSPs performing MCD actions in their objectives of defending DOD systems, applications, and data hosted in the cloud. Specific cyberspace defense actions include:
  - Protect the DISN via the BCAP.
  - Provide timely access to BCD-collected indications and warnings relevant to organizations performing MCD actions.
  - Support DCD actions to identify correlations between related events or incidents that impact multiple Mission Owners, CSOs, or CSPs.
- **Mission Cyberspace Defense (MCD) Actions:** The primary objective of organizations that perform MCD actions is to defend Mission Owners' systems, applications, and data

hosted in the cloud. MCD actions are performed by CSSPs on behalf of their organic organizations and subscribers. Specific cyberspace defense actions include:

- Analyze cyber incidents and events for Mission Owners.
- Monitor, protect, and defend Mission Owners' cloud-based systems, applications, and virtual networks in the CSP's CSOs infrastructure.
- Monitor, protect, and defend Mission Owners' cloud-based data in the CSO.
- Defend all connections to the CSO, whether via BCAP, VPN, IAP, direct internet access to public servers, or other.
- Monitor privileged actions (e.g., cloud management or Mission Owner application administration) and monitor for events or incidents against the Mission Owner applications (e.g., Structured Query Language [SQL] injection).
- Support DCD efforts to identify correlations between related events or incidents that impact multiple Mission Owners, CSOs, or CSPs.
- Ensure internal DOD communications are established between all entities, which include the Mission Owner and other organizations performing MCD and BCD actions.
- Provide visibility and awareness of cyber incidents or events impacting Mission Owner systems, applications, virtual networks, and data to JFHQ-DODIN.

6.2 Cyber Incident Reporting and Response

The CSSP contracted to perform MCD actions will be the DOD point of contact to which the CSP's operational entity will coordinate responses to incidents affecting the security posture of the CSP and the CSP's cloud service.

- For CSOs supporting **Impact Levels 2 to 5** that are multitenant or shared across federal agencies outside of the DOD, incidents will be reported to Department of Homeland Security (DHS) US-CERT as well as the CSSP contracted to perform MCD actions.
- For CSPs supporting **Impact Levels 4 to 6** that provide dedicated infrastructure to the DOD, incidents regarding that infrastructure and CSOs will not be directly reported to the CSSP contracted to perform MCD actions nor to US-CERT. USCYBERCOM/JFHQ-DODIN, upon receiving reports for these impact levels, will coordinate with US-CERT and other entities as appropriate.

Corresponding Security Controls: IR-4, IR-5, IR-6.

6.2.1 Incident Response Plans and Addendums

- The CSP will provide their approach to fulfilling DOD Cyberspace Defense integration requirements either as part of their Incident Response Plan or through an Incident Response Plan Addendum.
- The CSP will make their plan or addendum available to DISA for review and approval as a condition of its PA and inclusion in the DOD Cloud Service Catalog.
- The CSP will update and deliver the Incident Response Plan Addendum (if used) in conjunction with updates and deliveries of their Incident Response Plan, as required by the FedRAMP selected security control IR-1.

- The CSP must specifically address cyber incidents and data breaches, where a "breach" or cyber incident includes the loss of control, compromise, unauthorized acquisition, unauthorized access, or any similar term referring to situations where any unauthorized person has access or potential access to government data, whether in electronic or nonelectronic form, for any unauthorized purpose.
- The CSP must ensure the plan or addendum addresses all incidents regardless of the time, day, or location of the incident and must provide for notice to the government of any breach of its data. The plan or addendum must incorporate any other policies or procedures the government may require to be followed in the event of an incident, including but not limited to the following:
  - To whom within the government the incident will be reported in accordance with the incident reporting process defined in Section 6.5.3, Incident Reporting Mechanism.
  - Specific steps to be taken to mitigate or remedy the incident, including time periods for taking such steps (e.g., reporting of Personally Identifiable Information [PII] data breaches within one hour).
  - How and under what circumstances any individuals or entities affected by an incident will be notified and by whom.
  - Any other special instructions for handling computer security incidents affecting or potentially affecting U.S. government data consistent with guidance and policy directives issued by DOD, NIST, US-CERT, and CNSS for incident management, classification, and remediation; or other applicable law, regulation, order, or policy.

Corresponding Security Controls: IR-8.

6.2.2 Information Requirements, Categories, Timelines, and Formats

These requirements are applicable to all systems at all information Impact Levels. The CSP must follow these requirements when integrating with DOD organizations performing CSSP.

- Initial incident reports must be submitted within one hour of discovery with follow-on information provided as available.
  - Initial reports may be incomplete to facilitate communication and teamwork between the CSP and the organizations performing MCD/BCD actions. CSPs should balance the necessity of timely reporting (incomplete reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.
- Incident notifications should include a description of the incident and as much of the following information as possible.
  - Contract information, including the contract number, USG Contracting Officer contact information, contract clearance level, etc.
  - Contact information for the impacted and reporting organizations as well as the MCD.
  - Details describing any vulnerabilities involved (i.e., CVE identifiers).
  - Date/time of occurrence, including time zone.
  - Date/time of detection and identification, including time zone.

- Related indicators (e.g., hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures).
- Threat vectors, if known (refer to Threat Vector Taxonomy and Cause Analysis flowchart within the US-CERT Federal Incident Notification Guidelines).
- Prioritization factors (i.e., functional impact, information impact, and recoverability as defined in the flowchart within the US-CERT Federal Incident Notification Guidelines).
- Source and destination IP address, port, and protocol.
- Operating system(s) affected.
- Mitigating factors (e.g., full disk encryption or two-factor authentication).
- Mitigation actions taken, if applicable.
- System function(s) (e.g., web server, domain controller, or workstation).
- Physical system location(s) (e.g., Washington, DC, Los Angeles, CA).
- Sources, methods, or tools used to identify the incident (e.g., IDS, IPS and audit log analysis).
- Any additional information relevant to the incident and not included above.

6.2.3 Incident Reporting Mechanisms

DOD CSSPs will report all incidents using the Joint Incident Management System (JIMS) in accordance with normal DOD processes.

- Commercial CSPs supporting **Impact Level 2/4/5** will report all incidents via the online DIB Cyber Incident Collection Format (ICF). Use of the online format is preferred. Access to this format requires a DOD-approved medium assurance External Certificate Authority (ECA) certificate. If unable to access this format, call (877) 838-2174 or email: DCISE@DC3.mil.
  - The CSP must include the DOD missions affected by the incident when distributing this report (the DOD Mission Owners and Security POCs [CSSPs] and other entities that might have a role, such as contract managers, etc.). Once the report is received, the CSSP performing MCD actions will initiate the DOD reporting process via JIMS.
- Commercial CSPs supporting **Impact Level 6** will report all incidents to the organization performing MCD actions using SIPRNet email or secure phone/fax to report and coordinate incidents as specified.

Existing notification mechanisms of a CSP that are already in place to communicate between the CSP and its Mission Owners for some or all classes of Cyberspace Defense information may be used, if those mechanisms demonstrate a level of assurance equivalent to the listed encrypted mechanisms for the confidentiality and integrity of the information.

Corresponding Security Controls: IR-6, IR-8.

6.2.4 Support for Law Enforcement/Criminal Investigation

Incident information must be gathered and handled in a manner that will support legal prosecution if needed. This information must be protected from alteration from the time it is captured until it is

no longer needed. Support for forensics is shared between the Mission Owner and the CSP to various degrees depending on the service type.

Mission Owners must reflect these requirements in their contract/SLA with the CSP delineating specific responsibilities between the CSP and Mission Owner/CSSP performing MCD.

Corresponding Security Controls: IR-4, IR-5(1)

Analysis results for Mission Owners can be shared with the CSP if permissible and the appropriate communication channels exist.

Corresponding Security Controls: SI-3 (10).

Requirements in the following subsections apply to all information Impact Levels 2 through 6.

6.2.4.1 Incident Information Collection, Preservation, and Protection

- The CSP must capture, preserve, and protect images and state of all known affected systems/servers/workstations supporting the CSO and the customer. This includes system logs, volatile memory captures, and hard drive (physical or virtual) images.
- The CSP must preserve and protect all relevant network logs and all available network monitoring/packet capture data. This information must be collected as soon as possible after the discovery.
- For IaaS, when a Mission Owner discovers a cyber incident has occurred within their systems/applications/virtual networks, they will work with their organization performing MCD actions and CSP to capture, preserve, and protect images and state of all known affected virtual machines that they manage, as well as any network logs and network monitoring/packet capture data generated by their virtual network(s). This includes system logs, volatile memory captures, and virtual hard drive images. While the virtual hard drive image of a compromised VM is typically easy to preserve as a new image is placed into service, tools run on the compromised VM before it is shut down are typically used to capture and package the system logs and/or volatile memory and detailed procedures are followed.
- For PaaS and SaaS, it may be unlikely that the Mission Owner will be able to run the tools necessary to capture and preserve the information needed for forensics described above; however, the CSP must provide the required tools/capabilities to fulfill the preservation requirements for their CSO.
- For PaaS, if the Mission Owner manages their contracted servers, operating system, or platform applications, it is their responsibility to capture, preserve, and protect functions in coordination with their organization performing MCD actions on their own or using tools provided by the CSP. If the CSP manages the CSO servers, operating system, or platform applications, the CSP must perform the capture, preserve, and protect functions. The CSP will then create a dual report to share their results with the Mission Owner and CSSP.
- Under SaaS, the CSP must perform the capture, preserve, and protect functions. The CSP will then share their results with the Mission Owner's CSSP.

- The CSP must provide an automated capability that supports incident capture and protection from modification or deletion, which must support the CSP's investigation of incidents within their own infrastructure and in customer's CSO environments. An interface to the capability must be made available to the customer in support of the customer's incident response activities as needed in their environments within the CSO. All such automation must capture the information in a manner that segregates captured information by customer such that non-DOD or non-federal information is not revealed to the incident response team or investigators. Likewise, the information relating to the government environment must be segregated from the information captured from the CSP's underlying infrastructure. Once the information is captured, the automation must create one or more hashes of the data so changes to it can be detected. The automation must then encrypt the data to preserve its confidentiality and integrity. Captured information from the CSP's underlying infrastructure will be encrypted separately from the information captured from the government's environment. Encryption keys will be provided to the forensics analysists and stored in such a manner that only the government has access to the keys for the information captured from the government's environment and the CSP has access to captured data from the CSP's underlying infrastructure.

Corresponding Security Controls: IR-4, IR-5(1), IR-8, SI-12.

6.2.4.2 Supporting Chain-of-Custody Investigations

According to NISTIR 8006, chain-of-custody is defined "in legal contexts as the chronological documentation of evidence handling, which is required to avoid allegations of evidence tampering or misconduct." If the incident was maliciously caused by an individual, maintaining the chain of custody over the information is critical to being able to legally reprimand or prosecute the responsible individual or organization.

To support Law Enforcement/Counter-Intelligence (LE/CI) investigations, the chain-of-custody of the captured data should be documented from end-to-end, person-to-person starting when the incident investigation begins. The individual who captures each piece or portion of the information initiates this documentation and everyone that subsequently handles the information or media containing it must continue the documentation. Chain-of custody forms are available from law enforcement. While chain-of-custody documentation is important and recommended, initiating the chain-of-custody forms and procedures may only be required if the incident warrants the notification of law enforcement. In that case, the chain-of-custody forms will be initiated by law enforcement officers. If requested or subpoenaed, the CSP will make their employees available to provide attestation either via affidavits or expert testimony on the CSP's chain-of-custody and forensic data capture/collection methods.

Corresponding Security Controls: SI-12.

6.2.4.3 Digital Forensics Support by CSP Toward PA Award

CSPs will be evaluated for their ability to support the requirements above that are incumbent upon the CSP and for their ability to support requirements that are incumbent upon the Mission Owner, particularly in system image and state preservation. This includes capabilities and tools to support

the capture and preservation of system logs, volatile memory captures, and hard drive (physical or virtual) images by the Mission Owner or CSP.

- The CSP must document their capability to support digital forensics in their Security Plan. CSP forensics support capabilities and their acceptability will be documented in the information supporting the PA.

6.3 Warning, Tactical Directives, and Orders

USCYBERCOM or JFHQ-DODIN disseminates Warnings, Tactical Directives, and Orders to the organizations performing BCD and MCD actions. The organizations performing BCD and MCD actions will analyze them for their applicability to individual Mission Owners and CSPs, and then, as appropriate and applicable, communicate the requirements to these same Mission Owners and CSPs.

- CSPs will coordinate with the organizations performing MCD actions and Mission Owners to implement directives and countermeasures in compliance with timelines identified. Upon completion of actions, the organization(s) performing MCD and BCD actions will report compliance back to JFHQ-DODIN and USCYBERCOM.
- CSPs must be able to receive, act on, and report compliance with directives and notifications sent by the organization performing MCD actions on behalf of the Mission Owner as required by FedRAMP selected security control SI-5.

6.4 Continuous Monitoring/Plans of Action and Milestones (POA&Ms)

Understanding existing vulnerabilities and risks within the enterprise is a key component in performing effective Cyberspace Defense analysis.

- CSPs will develop vulnerability reports and POA&Ms as part of continuous monitoring requirements and will make available to DISA's cloud services support team and subsequently to the organizations performing MCD and BCD actions for their collective use in providing Cyberspace Defense.
- CSPs must mitigate High and Critical risk findings within 30 days and Moderate findings within 90 days.

Corresponding Security Controls: CA-5, CA-7.

6.5 Notice of Scheduled Outages

Planned outages affecting mission systems are to be coordinated through the Mission Owner, with the goal of minimizing impacts to the operational community.

- CSPs must notify all affected organizations performing MCD actions of scheduled outage under their control when an outage starts and upon return to service.
- The organization performing MCD actions must then report outages or changes that affect more than one mission environment to the organization performing BCD actions.
- Mission Owners and mission administrators are responsible for the same notifications to the organizations performing MCD actions when the scheduled outage is under their control.

6.6 PKI for Cyberspace Defense Purposes

This section outlines requirements for establishing trusted identities for CSP personnel communicating securely with DOD Cyberspace Defense personnel. Once an incident is reported, if digitally signed or encrypted email is to be used as the subsequent communications method, DOD PKI certificates will be required as follows:

- CSPs serving **Impact Levels 2 through 5** must have either a DOD PKI certificate (strongly preferred) or a DOD-approved PKI credential for each person that needs to communicate with DOD via encrypted email. For more information on DOD-approved credentials, refer to the Cyber Exchange PKI/ECA web page and PKI/PK Enabling (PKE) web page. Equivalent alternative measures will be assessed on a case-by-case basis.
- CSPs serving **Impact Level 6** must already have SIPRNet tokens/NSS PKI certificates for their system administrators by virtue of the connection to SIPRNet. Incident response and Cyberspace Defense personnel will use SIPRNet tokens/certificates to communicate with DOD via encrypted email.

6.7 Defense Industrial Base Cybersecurity/Information Assurance (DIB CS/IA)

The DIB CS/IA is a program to enhance and supplement DIB participants' capabilities to safeguard DOD information that resides on, or transits, DIB unclassified information systems. Under this public/private cybersecurity partnership, DOD and participating DIB companies share unclassified and classified cyber threat information, best practices, and mitigation strategies.

Eligible CSPs are encouraged to join the voluntary DIB CS/IA program to facilitate their protection of infrastructure that hosts higher-value DOD data and systems.

6.8 Insider Threat Program

Organizations handling classified information are required, under Executive Order 13587 and the national policy on insider threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and nontechnical information to identify potential insider threat concerns.

Mission Owners that lease, own, or use NSS must ensure the CSP implements the Directive and the Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated 21 November 2012.

APPENDIX A. REFERENCE AND RESOURCES

1. DOD Cloud Authorization Services Catalog.
https://DOD365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/sitepages/csocatalog.aspx
(DOD CAC/PKI required)
2. FedRAMP website.
https://www.fedramp.gov/
3. Public Law 93-579, as codified at 5 U.S.C. 552a, Privacy Act of 1974.
http://www.archives.gov/about/laws/privacy-act-1974.html
4. Public Law 104-191, Health Insurance Portability and Accountability (HIPAA) Act of 1996
http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html
5. Public Law 83-703, Atomic Energy Act of 1954.
https://www.govinfo.gov/content/pkg/COMPS-1630/pdf/COMPS-1630.pdf
6. 22 Code of Federal Regulations (CFR), 22 CFR 120.15 – US Persons, 120-16 – Foreign persons.
https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec120-15.pdf
7. 22 Code of Federal Regulations (CFR), 22 CFR 120.17 – Export.
https://www.gpo.gov/fdsys/pkg/CFR-2004-title22-vol1/pdf/CFR-2004-title22-vol1-sec120-17.pdf
8. 22 Code of Federal Regulations (CFR), 22 CFR 120.-130 International Traffic in Arms Regulations Part 123 - Licenses for the Export of Defense Articles.
https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120?toc=1
9. 8 U.S. Code § 1408 - Nationals but not citizens of the United States at birth.
https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12-subchapIII-partI-sec1408.pdf
10. Executive Order 13526: Classified National Security Information, dated 29 December 2009.
http://www.archives.gov/isoo/policy-documents/cnsi-eo.html
11. Executive Order 12829 – National Industrial Security Program, January 1993.
https://www.archives.gov/isoo/policy-documents/eo-12829-with-eo-13691-amendments.html
12. Executive Order 13556 - Controlled Unclassified Information.
https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information
13. EO 12958, Classified National Security Information (April 17, 1995) as amended by EO 13691.
https://www.archives.gov/isoo/policy-documents/eo-12829-with-eo-13691-amendments.html
14. 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry.
https://www.govinfo.gov/app/details/CFR-2022-title48-vol1/CFR-2022-title48-vol1-part4-subpart4-4
15. Federal Acquisition Regulations (FAR) Section 52.204-2 - Security Requirements.
https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf

16. NIST FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

17. NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011.
https://www.nist.gov/publications/nist-cloud-computing-reference-architecture

18. NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, dated September 2022.
SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

19. NIST SP 800-59: Guideline for Identifying an Information System as a National Security System, dated August 2003.
http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf

20. NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, dated October 2008.
http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

21. NIST SP 800-88, Revision 1: Guidelines for Media Sanitization, dated September 2012.
https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

22. NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010.
http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

23. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011.
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

24. NIST SP 800-145: The NIST Definition of Cloud Computing, dated September 2011.
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

25. NIST SP 800-37, Revision 2: Guide for Applying the Risk Management Framework to Federal Information Systems, dated December 2018.
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

26. NIST SP 800-171, Revision 2: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, dated Feb 2020, update January 2021.
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

27. CNSS Instruction 4009: Committee on National Security Systems (CNSS) Glossary, dated 2 March 2022.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm

28. CNSS Instruction 1253: Security Categorization and Control Selection for National Security Systems, dated 01 August 2022.
https://www.cnss.gov or www.cnss.gov/cnss/issuances/Instructions.cfm

29. DOD Chief Information Officer, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014.
http://dl.cyber.mil/cloud/pdf/commercial_cloud_computing_services.pdf

30. DOD Instruction 8500.01: Cybersecurity, dated 14 March 2014, change 1 7 October 2019.
https://www.esd.whs.mil/portals/54/documents/dd/issuances/DODi/850001_2014.pdf

31. DOD Instruction 8510.01: Risk Management Framework (RMF) For DOD Information Technology (IT), dated 19 July 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/851001p.pdf
32. DOD Instruction 8520.03: Identity Authentication for Information Systems, dated 19 May 2023. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/852003p.pdf
33. DOD Instruction 8551.01: Ports, Protocols, and Services Management (PPSM), May 31, 2023. https://www.esd.whs.mil/portals/54/documents/dd/issuances/DODi/855101p.pdf
34. DOD Instruction 8410.01, Internet Domain Name Use and Approval, Change 1 June 4, 2021. https://www.esd.whs.mil/portals/54/documents/dd/issuances/DODi/841001p.pdf
35. DOD Instruction 8530.01, "Cybersecurity Activities Support Procedures" dated May 31, 2023. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODm/853001p.PDF?ver=BFUagWhkQR8fBXzxRjIqxQ%3D%3D
36. DOD Instruction 8582.01, Security of Non-DOD Information Systems Processing Unclassified Non-Public DOD Information dated 9 December 2019. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/858201p.pdf?ver=2019-12-09-143118-860
37. DOD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, change 1 5 December 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/832007p.pdf?ver=2019-06-06-091932-567
38. National Industrial Security Program Part 117 of 32 CFR. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
39. DOD Instruction 5200.01: DOD Information Security Program and Protection of SCI, change 2 dated 01 October 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/520001p.PDF?ver=cF1II-jcFGP6jfNrnTr8lQ%3d%3d
40. DOD Manual 5200.01 Vol 1: DOD Information Security Program: Overview, Classification and Declassification, dated February 2012. https://www.esd.whs.mil/directives/issuances/DODm/
41. DOD Manual 5200.01 Vol 2: DOD Information Security Program: Marking of Classified Information, dated March 2013. https://www.esd.whs.mil/directives/issuances/DODm/
42. DOD Manual 5200.01 Vol 3: DOD Information Security Program: Protection of Classified Information, dated March 2013. https://www.esd.whs.mil/directives/issuances/DODm/
43. DOD Instruction 5200.02: DOD Personnel Security Program (PSP), Change 1 dated September 2014. https://www.esd.whs.mil/Directives/issuances/DODi/
44. DOD Manual 5200.02: Personnel Security Program, dated February 1996. https://www.esd.whs.mil/directives/issuances/DODm/

45. CJCSM 6510.01B: Chairman of the Joint Chiefs of Staff Manual: Cyber Incident Handling Program, dated 10 July 2012. (Current as of 18 December 2014). https://www.jcs.mil/Library/CJCS-Manuals/

46. DCSA Facility Clearance Branch. https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Facility-Clearances/

47. DOD ECA PKI Certificate. https://public.cyber.mil/pki-pke and https://cyber.mil/pki-pke (DOD CAC/PKI required)

48. FedRAMP Control Specific Contract Clauses v3, December 8, 2017. https://www.fedramp.gov/

49. Defense Information Systems Agency, the Security Technical Implementation Guide (STIG) Home Page. https://public.cyber.mil/stigs and https://cyber.mil/stigs (DOD CAC/PKI required)

50. Defense Information Systems Agency, DOD Cloud Services Support website. https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/cloud-service-support

51. OPM Position Designation Tool. https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/

APPENDIX B. GLOSSARY

B.1. Cloud Terminology

Cloud Service Provider (CSP): An organization that provides cloud services. May be commercial, government, or DOD.

- **Commercial CSP:** A nonfederal government non-DOD organization offering cloud services to the public and/or government customers as part of a business venture, typically for a fee with the intent to make a profit.
- **Federal Government CSP:** A federal government organization offering cloud services, which may be owned and operated by the federal government or a contractor for the benefit of the federal government.
- **DOD CSP**: A DOD organization offering cloud services, which may be owned and operated by DOD or a contractor for the benefit of the DOD.
- **Non-DOD CSP:** A commercial CSP or federal government CSP.

Cloud Service Offering (CSO): Refers to a CSP's product or service offering. A CSO is the actual IaaS, PaaS, or SaaS solution available from a CSP. A CSP may provide multiple CSOs (e.g., Microsoft O-365 [SaaS] and Azure [I/PaaS]). CSO also refers granularly to optional services or software available within any of the service types (e.g., one or more specific database applications optionally available for customer usage under PaaS).

- **Infrastructure as a Service (IaaS)**: As defined in NIST SP 800-145, "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."
- **Platform as a Service (PaaS)**: As defined in NIST SP 800-145, "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."
- **Software as a Service (SaaS):** As defined in NIST SP 800-145, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings."

Community Cloud: A multitenant cloud in which services are provided for the exclusive use of a specific group or type of independent customer organizations.

Federal Government Community Cloud: A community cloud offered for use by multiple federal government organizations (which include the DOD). Resources providing the cloud services must be dedicated to federal government use and require physical separation from nonfederal customers.

Private Cloud: A single or multitenant cloud in which services are provided for the exclusive use of a specific customer organization.

DOD Private Cloud/CSO: A DOD Community Cloud or CSO in which services are provided for the exclusive use of one or more DOD customer organizations; supporting multiple DOD tenants or DOD-sponsored tenants in the same cloud. The DOD maintains ultimate authority over the use of the cloud services, and any non-DOD use of services must be authorized and sponsored through the DOD. Resources providing the cloud services must be dedicated to DOD use and have physical separation from resources not dedicated to DOD use.

DOD Cloud Service Catalog: The repository of all CSOs that have been awarded a DOD PA and have security packages available for DOD components to leverage.

DOD component: A DOD Service or Agency including their subelements, commands, or organizations.

DOD Off-Premises: A facility (building/container) or IT infrastructure that is NOT physically or virtually on DOD owned or controlled property (i.e., on-premises physically or virtually).

DOD On-Premises: A facility (building/container) or IT infrastructure that is physically on DOD owned or controlled property. It is within the protected perimeter (walls or "fence line") of a DOD installation (i.e., Base, Camp, Post, or Station [B/C/P/S] or leased commercial space) that is under the direct control of DOD personnel and DOD security policies.

DOD Virtually On-Premises: An IT infrastructure located in a physically off-premises location such as a federal government or commercial data center (i.e., facilities under the direct control of non-DOD personnel using non-DOD security policies) may be considered virtually on-premises under specific conditions. These conditions apply certain physical security controls and extend the DISN accreditation boundary. This construct virtually extends the DOD protected perimeter or "fence line" around the infrastructure.

Federal Information System: An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. 40 USC 11331, Subchapter III, sec 11331, page 209, para g.

Mission Owner: Entities such as IT system/application owner/operators or program managers within the DOD components/Agencies responsible for instantiating and operating one or more information systems and applications who may leverage a CSP's CSO in fulfillment of their IT missions. In this context, the Mission Owner is not the DOD Enterprise or DOD component/Agency Enterprise, even though these entities may control and have oversite for Component/Agency level policies and the Mission Owner's acquisitions. The Mission Owner is also responsible to the Information Owner and the information system's AO. The information owner, in addition to owning the information and all associated derivatives, is responsible for ensuring the

data that is migrated to the cloud is at the appropriate security level having the approval of their Risk Management Executive/AO.

B.2. General Terminology and Acronyms

Security control (control/control enhancement): NIST SP 800-53 Security and Privacy controls and their enhancements, which are selected and assembled in various baselines and overlays.

CSM: Cloud Security Model. The CSM is the document that preceded the Cloud Service Provider SRG and has since been deprecated.

CSSP: Cybersecurity Service Provider. Defined in DODI 8530.01, Cybersecurity Activities Support to DOD Information Network Operations.

Dedicated infrastructure: Refers to the cloud service infrastructure being dedicated to serving a single customer organization or a specific group of customer organizations (e.g., a specific community).

Cyber incident: Actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. Refer to "incident."

JAB: Joint Authorization Board. The primary governance and decision-making body for the FedRAMP program

Mission Owner: A DOD Cloud Consumer. As defined in NIST SP 500-292, "A cloud consumer represents a person or organization that maintains a business relationship with and uses the service from a cloud provider."

Provisional Authorization (PA): A preacquisition type of Risk Management Framework Information System Authorization used by DOD and FedRAMP to prequalify commercial CSOs to host federal government and/or DOD information and information systems. PAs are to be used by federal and DOD Cloud Mission Owners during source selection and subsequent system authorization under RMF.

RMF: Risk Management Framework. Defined in NIST SP 800-37. RMF is a six-step risk-based approach to information system security, the purpose of which is compliance with various public laws, including FISMA. The RMF replaces the traditional certification and accreditation C&A processes.

APPENDIX C. ROLES AND RESPONSIBILITIES

Table C-1 provides a summary of the major roles and responsibilities in implementation of the Cloud Service Provider SRG.

Table C-1: Roles and Responsibilities

Role	Responsibility
DISA	• Provide SRGs and STIGs for DOD cloud computing. • Assess CSP's Service Offerings and 3PAO results for consideration in awarding a DOD PA. • Issue DOD Provisional Authorizations. • Develop and maintain a DOD BCAP. • Provide BCD capabilities. • Provide technical support for the DOD CIO's role on the FedRAMP Joint Authorization Board. • Provide a catalog of DOD cloud services. • Maintain a registry of DOD components using commercial cloud services. • Support the DODIN Waiver Process. • Receive CSP's continuous monitoring products and passes them to the appropriate entities within DOD. • Serve as the DOD CSSP certifier.
Cloud Service Provider (CSP)	• Commercial vendor or federal organization offering or providing cloud services (includes DOD CSPs). • Provides one or more CSOs for mission use. • Provides cybersecurity services for their infrastructure and service offerings.
Cloud Access Point (CAP)	• Provided by DISA or another DOD component. • Protect DOD missions from vulnerabilities or risk that may affect operations in a CSP environment . • Provide perimeter defenses and sensing for applications hosted in the commercial cloud service.
DOD Chief Information Officer (DOD CIO)	• Official approving authority for all CAPs.

Role	Responsibility
FedRAMP Joint Authorization Board (JAB)	• Reviews CSP security assessment packages under the FedRAMP program . • Grants FedRAMP PAs. • Ensures FedRAMP PAs are reviewed and updated regularly. • Approves accreditation criteria for 3PAOs.
Third-Party Assessment Organizations (3PAO)	• Accredited by American Association for Laboratory Accreditation (A2LA) and with final approval by FedRAMP PMO. • Contracted by CSP. • Independently performs security assessments of a CSP cloud offering and creates security assessment package artifacts in accordance with FedRAMP requirements. • May perform continuous monitoring of CSP systems. • May independently assess a CSP's compliance with DOD FedRAMP+ security controls and other requirements.
DISA Cloud SCA	• May independently assess a CSP's compliance with DOD FedRAMP+ security controls and other requirements if not performed by a 3PAO. • May assess a CSP's compliance with FedRAMP security controls for DOD CSPs if not done by another DOD SCA. • May assess a CSP's compliance with FedRAMP security controls for commercial CSPs undergoing a DOD assessment outside of FedRAMP if not done by another DOD SCA. • Advises the DISA AO regarding PA award through the assessment of CSP SARs and the development of a Certification Recommendation. • Serves as FedRAMP technical advisor to the DOD CIO in the role as JAB tri-chair.
DOD Cloud SCA (other than DISA)	• May assess a CSP's compliance with FedRAMP and FedRAMP+ security controls for DOD or non-DOD CSPs undergoing a DOD assessment outside of FedRAMP (if not done by DISA) toward awarding an DOD PA and component Agency ATO.
Authorizing Official (AO)	• DISA AO: Official approving PA for a CSP's Service Offerings for DOD use. • Component AO: Approves ATOs for Mission Owner's systems/applications. Reviews PA documentation to understand residual risk.

Role	Responsibility
Mission Owner (DOD Cloud Customer)	• DOD entity that acquires cloud services in support of its mission. • Reviews DOD PA documentation to understand residual risk. • Performs assessment to issue ATO for their mission systems/applications. • Ensures MCD Service Provider is identified and funded . • Performs endpoint Cyberspace Defense for their mission systems/applications. • Ensures CSP requirements for Cyberspace Defense and other SRG requirements are included in cloud contracts. • Registers ports and protocols with the Ports, Protocols, and Services Management (PPSM) Office.
United States Computer Emergency Readiness Team (US-CERT)	• Receives incident reports from CSP as mandated by FedRAMP. • Coordinates across non-DOD agencies.
Computer Network Defense Service Provider (CDSP)	• Provides Cyber Defense services and C2 direction addressing the protection of the network, detection of threats, and response to incidents.
Cybersecurity Service Provider (CSSP)	• Provides cybersecurity services for the protection of the network, detection of threats, and response to incidents.
Organizations Performing Boundary Cyberspace Defense (BCD) Actions • DOD CSSPs	• Monitor and defend the connections to/from off-premises CSPs at the BCAP. • Provide cross-CSP analysis capabilities or entities . • Communicate with organizations performing DCD, BCD, and MCD actions. • Provide MCDs timely access to BCD-collected indications and warnings relevant to MCD subscribers.
Organizations Performing Mission Cyberspace Defense (MCD) Actions • DOD CSSP	• Provide Cyberspace Defense services to specific Mission Owner's systems/applications and virtual networks. • Serve as the DOD Cyberspace Defense point of contact for the Mission Owner. • Communicate with organizations performing DCD, BCD, and MCD actions and Mission Owners.

APPENDIX D. FEDRAMP+ SECURITY CONTROLS AND PARAMETER VALUES

Table D-1 lists the required FedRAMP+ security controls parameter values and the FedRAMP security control for which DOD requires adjustment. These security controls and associated parameter values are published here as a benchmark for CSPs and will be used for CSP assessment toward receiving a PA. **It is not a complete list of all security controls that a CSP must meet**.

For Level 5, National Security Systems will require the additional CNSSI 1253 controls for those systems. The parameters will be the DOD RMF TAG value, CNSSI 1253 value if no DOD RMF TAG value exists, or AO tailored value unless designated by this document.

For Level 6, the application of the CNSSI 1253 Classified Information Overlay will modify some of the values of security control presented below as well as other security controls not listed. Overlay values take precidence.

DOD Componets/Mission Owners must use, define, and/or tailor the parameter values for the applications they instantiate in IaaS/PaaS cloud services in accordance with the values defined by the DOD RMF TAG. DOD/FedRAMP predefined and CSP-defined parameter values assessed for DOD PA award are inherited by the Mission Owners' systems/applications. If the Mission Owner needs alternate values for these inherited values, they must be negotiated with the CSP and reflect the change in their SLA/contract.

In addition to parameter values required for the implementation of FedRAMP+ security controls, Table D-1 contains security controls where the value is nonexistent or requires adjustment. The controls listed that are part of the FedRAMP baseline must use the value listed in the table.

Table D-1: FedRAMP+ Additions/Adjustments to Parameter Values for FedRAMP+ Security Controls/Enhancements

Control	Parameter Values	Impact Level
AC-7	For privileged users, DOD limits to three unsuccessful attempts and requires an administrator to unlock. For nonprivileged users, if rate limiting, DOD will allow 10 attempts with the account automatically unlocked after 30 minutes. If rate limiting is not used, normal DSPAV will be required.	IL4, IL5, IL6
AU-5(1)	CSP/CSO may use FedRAMP value.	IL4, IL5, IL6
CM-7(5)	DSPAV must be used.	IL4, IL5, IL6
IA-5(1)	DSPAV must be used.	IL4, IL5, IL6
PE-15	DSPAV must be used.	IL4, IL5, IL6
PS-3(4)	All information systems. Users: U.S. citizens, U.S. nationals, or U.S. persons, foreign personnel as allowed by current DOD polices with AO approval. Administrators: U.S. citizens, U.S. nationals, or U.S. persons.	IL4, IL5, IL6
MA-5(1)	DSPAV must be used.	IL4
MA-5(2)		IL6

Control	Parameter Values	Impact Level
MA-5(3)		IL6
MA-5(4)		IL6
MA-5(5)		IL4, IL5, IL6
MA-6	CSP/CSO may use FedRAMP value.	IL4, IL5, IL6
PS-4	CSP/CSO may use FedRAMP value.	IL4, IL5, IL6
SA-4(5)	DSPAV must be used.	IL4, IL5, IL6
SA-9(1)	DSPAV must be used.	IL4, IL5, IL6
SA-9(3)	DSPAV must be used.	IL4, IL5, IL6
SA-9(5)	SA-9 (5)-1 [information processing, information or data, AND system services]. SA-9 (5)-2 [U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction]. SA-9 (5)-3 [all data, systems, or services].	IL4, IL5, IL6
SA-9(6)		IL4, IL5, IL6
SA-9(7)		IL4, IL5, IL6
SA-9(8)		IL4, IL5, IL6
SC-12(6)		IL4, IL5, IL6
SC-17	DODI 8520.02, Public Key Infrastructure (PKI) and Public Key Enabling (PKE).	IL4, IL5, IL6
SC-18		IL4, IL5, IL6
SC-18 (2)	DSPAV must be used.	IL4, IL5, IL6
SC-18 (3)	Supplemental guidance: For the protection of the infrastructure supporting a CSO, CSPs should apply this control to their organizational IT systems and the infrastructure supporting their CSO(s). For the protection of Mission Owners, their end users, and networks, CSP CSOs must not support the downloading of mobile code, which is deemed unacceptable to DOD. Refer to Section 5.11, Mobile Code, for more information.	IL5, IL6
SC-18 (4)	Software applications such as but not limited to email, scriptable document/file editing applications that support documents with embedded code (e.g., Microsoft Office applications/documents), etc. Prompting the user for permission.	IL5, IL6
SC-24	DSPAV must be used.	IL4, IL5, IL6
SC-46	DSPAV must be used.	If CDS is used